CLAUDIA JOHANA ZARATE ROJAS

Gestión de la seguridad de la información de datos personales en el derecho Informático

Maestría en Derecho Informático y de las Nuevas Tecnologías

Bogotá, D.C., Colombia

2020

UNIVERSIDAD EXTERNADO DE COLOMBIA

FACULTAD DE DERECHO

MAESTRIA EN DERECHO INFORMATICO Y DE LAS NUEVAS TECNOLOGIAS

Rector: **Dr. Juan Carlos Henao Pérez**

Secretaria General: **Dra. Martha Hinestrosa Rey**

Director Departamento: **Dra. Teresa Vargas Osorno**

Director de Tesis: **Dr. Daniel Peña Valenzuela**

Presidente de Tesis: **Dra. Teresa Vargas Osorno**

Jurado _____

Jurado _____

Jurado _____

Gestión de la seguridad de la información de Datos personales en el derecho Informático.

Tabla de contenido

Índice de Tablas

Índice de Gráficos

Gestión de la seguridad de la información de datos personales en el derecho Informático.

1. Introducción

La tecnología impone cada vez mayores retos para el contenido normativo, tal es el caso del tratamiento de los datos personales, que necesariamente se ven más expuestos, gracias al avance acelerado de las tecnologías de la información y las comunicaciones (Tics), ante este contexto, es importante que la legislación nacional, internacional, las buenas prácticas internacionales y nacionales aplicables y demás recursos normativos, marchen de forma consecuente, cubriendo las necesidades derivadas del presente escenario globalizado.

Es necesario hacer entonces, un recorrido por la legislación en materia de protección de los datos personales, en el marco de la seguridad que debe tener la información sensible y particular de los individuos de una sociedad, máxime cuando los recursos tecnológicos actualmente disponibles, conceden mayor oportunidad de vulnerar o acceder a este tipo de información.

A partir de allí, se tendrán las herramientas argumentativas para evaluar si dichos recursos, tanto normativos como corporativos cubren las necesidades de los usuarios en materia de protección y mínima exposición de su intimidad y demás derechos relacionados.

El presente trabajo de tesis de investigación tiene por objeto analizar los aportes e incidencia de la normatividad en la gestión de la seguridad de la información de datos personales en Colombia, proponiendo una base argumentativa efectiva, que sirva como elemento de construcción legislativa que ayude a cubrir las necesidades derivadas de este estudio.

Con el propósito de obtener los resultados esperados, se procederá a verificar la normatividad disponible sobre el tema objeto de estudio, por medio del análisis de contenido de las diferentes fuentes del derecho, que hacen referencia a la protección de datos personales.

En segundo lugar, se realizará una verificación de la percepción de los usuarios en cuanto a su conformidad o inconformidad respecto del trato de sus datos personales, por medio de un diagnóstico, producto del enfoque metodológico cuantitativo, a fin de establecer la viabilidad de unificación de conceptos y la necesidad de expedición de una normatividad específica frente a la gestión de la seguridad de la información de datos personales en el marco del derecho informático.

Los resultados esperados son la obtención de un análisis, que permita establecer la prospectiva en relación a un cambio legislativo, con respecto al tema en cuestión, que permita cubrir las necesidades jurídicas y se adecue a las necesidades de los ciudadanos y del contexto tecnológico.

2. Capítulo 1: Gestión de la seguridad de la información de Datos personales: Marco conceptual.

2.1.Datos personales, Nociones Básicas y Antecedentes

2.1.1. Nociones Básicas:

En el diccionario de la real academia de la lengua, los datos personales son definidos como: "*dato de carácter personal*" (**Real Academia Española, 2014**) es decir, cuya incumbencia es relativa únicamente a su titular, lo que desde la noción más básica sugiere un grado de reserva e intimidad.

Otro tipo de acepciones lo califican como información privada de personas fiscas, sujeta a su intimidad y que trata temas sensibles que podrían generar exclusión o afectar su vida cotidiana de llegar a ser de conocimiento público.

De acuerdo a la doctrina mundial, encontramos acepciones que relacionan directamente la protección de los datos personales con el derecho a la intimidad, como es el caso de Delgado Triana, que lo define como la protección que tiene el ciudadano frente a las injerencias, intromisiones, vistas, publicaciones, así como el empleo o comunicación de los mismos, que de uno u otro modo apropien vulneren o degraden la información personal **(Delgado Triana, 2007, pág. 41**).

Existen además opiniones como la de Francesco Riccobono, que lo lleva al ámbito de la libertad informática y habla de él, como un derecho que pertenece a la personalidad moral definido como el poder de disposición de los datos personales, el conocimiento de su utilización para el fin que ha sido autorizado (**Riccobono, 1991, pág. 6**).

La ley 1581 del 2012 (**Congreso de la República, 2012**), por su parte, los define como: "*Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables*" (Art 3)

Así, los datos personales refieren a toda la información o registros que puedan vincular o identificar a una persona, los cuales pueden ser desde el nombre, documento, dirección o teléfono, hasta datos que requieren manejo y protección más precisa como antecedentes judiciales, crediticios y médicos o también a hábitos de consumo, gustos u orientación sexual.

Tipos de datos personales:

Rivera Llano, en su aproximación a la sociedad actual, los derechos y la libertad informática, afirma que existen varios tipos de datos personales y que de acuerdo con su complejidad y nivel de vulnerabilidad para el sujeto de derecho de protección deben establecerse los mecanismos adecuados para la protección de la intimidad y la información personal **(Rivera Llano, 2008)**.

Según lo establecido por la Superintendencia de Industria y Comercio en su cartilla guía para la protección de datos personales **(Superintendencia de Industria y Comercio, 2017)**, la recolección de los mismos debe hacerse en atención a tres circunstancias que determinan su grado de protección:

Los datos íntimos y privados, los datos semiprivados y los públicos. La primera acepción hace referencia a aquellos datos cuya sensibilidad debe ser cuidada al extremo, pues dicha información solo interesa al titular y solo deben ser obtenidos cuando este así lo quiera o en una circunstancia que amenace su vida.

En cuanto a los datos semiprivados, se refiere a información privada que interesa al titular y a un determinado círculo de personas, las cuales tienen que pedir autorización para acceder a ellos, tal es el caso de la vida crediticia que administra data crédito.

Los públicos por su parte hacen referencia a información de interés general, cuya protección no se encuentra sometida a la autorización derivada de su exposición o uso como es el caso de la identificación.

Los datos personales se dividen también, de acuerdo a su naturaleza, complejidad u grado de intimidad y de acuerdo con la prioridad que dicte esta clasificación deben ser protegidos adecuadamente según el caso.

En relación a los datos de identificación primarios encontramos los datos que son sometidos a mayor exposición pública y que tienen que ver con: nombres y apellidos, dirección de residencia, teléfono fijo y móvil, fecha de nacimiento, edad, tipo y numero de documento de identidad, estado civil, nacionalidad, así como los cada vez más frecuentes ubicaciones tecnológicas como la dirección IP o el correo electrónico.

Están además, los datos patrimoniales o semiprivados, retomados en la Ley 1266 de 2008 o Ley de Habeas Data (**Congreso de la República, 2008)** que incluyen la información fiscal, datos crediticios, ingresos, egresos e información general sobre cuentas bancarias y movimientos financieros (Art 3. Lit g).

Frente a los datos laborales y académicos es decir la información sobre su trabajo y estudio respectivamente, como el puesto que se ocupa dentro de una organización empresarial o la trayectoria educativa y títulos, es importante resaltar lo señalado por Rivera llano (**Rivera Llano, 2008**), quien afirma que el nivel de importancia en la protección de datos personales dependerá en gran medida del acceso público o restringido que se promueva en el trato.

También encontramos los de salud y características personales que refieren a historia clínica, tipo de sangre, ADN y rasgos físicos particulares; Y por último los ideológicos que incluyen la filiación política, creencias religiosas y la pertenencia a grupos o corporaciones sociales de diferentes pensamientos, así como los de preferencias sexuales, modo de vida y origen étnico o racial.

2.2.Antecedentes.

2.2.1. Contexto mundial.

La primera referencia legal, se produjo en el año de 1948, en el marco de la Declaración Universal de los Derechos Humanos, que en su artículo 12 señala que: *"Toda persona debe ser protegida ante injerencias arbitrarias en su vida privada, familia, domicilio o correspondencia, así como de ataques contra su honra y su reputación"* (**Organizacion de Naciones Unidas, 1948**).

En el año de 1966, la Asamblea General de las Naciones Unidas, se pronunciaría al respecto en el Pacto Internacional de Derechos Civiles y Políticos, ratificando la posición frente a la protección de la intimidad de las personas, en el artículo 17 reforzando de esta forma lo plasmado en la Declaración Universal de Derechos humanos.

2.2.2. Contexto Europeo.

En Alemania en 1983, el Tribunal Constitucional Federal promovió una ley que busca proteger el derecho a la personalidad y a la dignidad humana, llamada la ley del censo, que resalta una vez más el derecho al libre desarrollo de la personalidad y a la dignidad humana, añadiendo además el derecho a la autodeterminación informativa (**Ley del Censo, 1983**), aspecto clave, en el camino legislativo europeo hacia la protección de la intimidad y los datos personales.

Más adelante, debido al desarrollo creciente de las llamadas tecnologías de las telecomunicaciones y la información y a la inmersión de estas en la privacidad de las personas, nace la idea de la protección de datos personales, en busca de cubrir la problemática y ofrecer una solución de protección de los derechos fundamentales.

De esta forma se generó la necesidad en Europa de garantizar la seguridad en la transferencia de datos entre los países (**Parlamento Europeo, 1995**), otorgando lineamientos para los responsables de manejo de datos en cualquier ámbito de aplicación.

Como se evidencia fue la legislación europea la que toma la delantera en materia de datos personales, constituyéndose como uno de los primeros referentes en esta materia, liderando el proceso de protección a la intimidad de las personas, generando un antecedente importante en el reconocimiento de este derecho, como de carácter fundamental y primario.

2.2.3. Contexto Norteamericano

En estados Unidos, en el año de 1974 se proclama la ley general Privacy Act, que busca que los estados, garanticen a todas las personas protección legal igualitaria, lo que había sido consignado con anterioridad en la Decimocuarta Enmienda (**Nieves Saldaña, 2011**), sin embargo, presentaba dificultades en cuanto a su alcance, pues no podía aplicarse al ámbito privado o estatal, manteniéndose limitado al ámbito federal.

Por primera vez se contemplaron protecciones legales que propendieran por la obligación de proteger los datos personales por medio del manejo exclusivo en casos en que el titular de los mismos, así lo autorizara.

A partir de allí, el país norteamericano ha proyectado y legislado sobre el asunto para diferentes sectores, entre los que se encuentran archivos de televisión por cable, archivos electrónicos, informes de naturaleza financiera (**Nieves Saldaña, 2011**), entre otros.

Lo anterior, si bien, puede llegar a ser beneficioso en el área específica, no cuenta con la adecuada supervisión, ni establece mecanismos de evaluación y control, además de que dicha fragmentación en la legislación requiere una continua renovación, dados los cambios propios del

contexto globalizado, máxime en un país que lidera el tema tecnológico, donde la protección está enfocada a la circundante a temas financieros y está más dirigido a la protección del patrimonio que al derecho fundamental que protege la intimidad de las personas

2.2.4. Contexto Latinoamericano

Con respecto a América Latina, el proceso ha sido un poco más lento, pues fue solo hasta el año 2003, en la Cumbre Iberoamericana de Jefes de Estado, que los mandatarios de 21 de los países de sur y centro américa (**CEPAL, 2010**), evidenciaron su preocupación con respecto a la necesidad de regular el derecho a la intimidad y la protección de datos personales, formalizándose de este modo la Red Iberoamericana de protección de datos, que cubría a todos los países miembros.

Paralelamente otros organismos internacionales como la ONU, procuraron establecer mecanismos para garantizar un marco normativo que aumentara la protección en temas específicos, como el contexto comercial y mercantil, en el marco del "Model Law on Electronic Commerce" emitido por la Comisión de las Naciones Unidas para el Desarrollo Mercantil Internacional (UNCITRAL) en el año de 1996 (**CEPAL, 2010)**, en donde entre otras cosas se regularon aspectos relacionados con la firma electrónica.

Por su parte, el Comité de Política del Consumidor de la Organización para la Cooperación y el Desarrollo Económico **(OCDE),** formulo en el año de 1999 los lineamientos para la protección al consumidor en el contexto del comercio electrónico, más adelante otras organizaciones supranacionales como la Organización de los Estados Americanos **(OEA),** manifestaron la importancia de proteger los datos personales y la privacidad de los ciudadanos, además de cuidar los proceso y procedimientos del flujo de información personal entre países.

Surgió entonces la resolución 2661/11 sobre protección de datos personales y el acceso a la información pública (**Piñar Mañas, 2006**), que todos los países miembros deben tener en cuenta debido a su filiación con el organismo y su ámbito de aplicación.

En relación con los países en su legislación interna, la mayoría de los estados latinoamericanos hace mención de la intimidad y su correspondencia con la salvaguardia de la información personal, sin embargo, solo México y Argentina han incluido en su articulado constitucional el derecho expreso a la protección de datos personales.

Así, Latinoamérica se ha visto relegado en materia de protección de datos personales, al no contar con las herramientas jurídicas adecuadas y las que se encuentran, no abordan de manera eficiente la problemática, no se le da la rigurosidad y el trato adecuado que deberían tener y lo más importante solo en casos excepcionales se reconoce como un derecho fundamental desligado de otros, que se consideran de mayor importancia.

2.2.5. Contexto Colombiano

En Colombia, la Constitución Política de 1991 hace referencia al derecho a la intimidad **(Congreso de la República, 1991),** tanto de la persona, como de la familia y lo que esto conlleva y bajo este marco constitucional se desarrolla el Habeas Data mediante la Ley 1266 del 31 de diciembre de 2008:

> *"Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones* **(Congreso de la República, 2008**).

De tal manera que se empieza a dar aplicación a un derecho autónomo que permite a todas las personas conocer, actualizar y rectificar los datos que se recolectan de ellas en bases de datos o archivos.

Partiendo de la normatividad antes señalada, el legislador se vio en la necesidad de dar reglamentación legal que permita la aplicación de la protección de datos personales de una manera concreta, por lo que expidió la Ley estatutaria 1581 de 17 de octubre de 2012 reglamentada por el Decreto 1377 del 27 de junio de 2013.

No obstante lo anterior, se encuentra escaso el alcance de dicha protección de datos personales y las políticas de privacidad que se establecen, por cuanto se constriñe la voluntad de los usuarios o clientes, pues se hace exigible en la mayoría de los casos la autorización del uso de los datos personales de manera indeterminada (**Superintendencia de Industria y Comercio, 2017**) en lo que se refiere a sus receptores para llevar a término una transacción y/o servicio.

Lo anterior con el fin de generar un ambiente de seguridad y protección al momento del tratamiento de los datos recolectados por los diferentes canales comerciales, donde existe la posibilidad de implementar alguna garantía que permita una mayor protección a la intimidad y desarrollo de la personalidad, bajo la aplicación del principio de libertad informático y/o autodeterminación informativa.

2.3.Importancia del derecho a la protección de los datos personales:

El punto de partida de los derechos fundamentales y la base del derecho constitucional de los pueblos es la dignidad humana, en la protección y salvaguarda de la misma se encarnan las calidades mínimas con las que toda persona debería poder vivir **(Remolina Angarita, 2013)**,

esta le proporciona valor al ser humano, por el solo hecho de serlo y le suministra características propias de su individualidad como ser racional y libre.

Debe agregarse además, la posición antropocéntrica de la concepción de estado y sociedad, que posiciona al hombre como eje de los fines sociales y estatales, portador de su lugar preponderante como protagonista del régimen constitucional **(Remolina Angarita, 2013)**, lo anterior reconoce que cada persona tiene un valor especial, con peculiaridades intrínsecas a su ser individual, que existe la diversidad y que esta debe ser respetada en el marco del estado social de derecho y de una democracia inclusiva.

Dicho ser individual, debe ser protegido en su intimidad, la información acerca de las particularidades en cualquier aspecto de su vida, deben ser valoradas y cuidadas, en sintonía con su dignidad humana, dicho de otra manera, la protección de los datos personales es primordial en la cotidianidad de los individuos y su protección jurídica y legal imperativa, en un contexto en el cual cada vez es más fácil acceder a la información privada.

Dada la importancia de la protección de los datos personales, la intimidad de los individuos y su conexión con la dignidad de ser humano **(Prado, 2012)**, el trato constitucional y legal, debe traducirse en un derecho fundamental y en la creación de mecanismos jurídicos para la imperiosa protección de todo lo que concierne a la información personal del hombre y su individualidad.

Así, el sujeto de derechos debe encontrar un marco legal que le permita decidir sobre su información personal, controlar quien la administra , además de disponer de forma individual sobre su uso correcto.

El ordenamiento jurídico debe conceder a las personas autonomía en lo que refiere a todo tipo de información sensible y personal **(Piñar Mañas, 2006)**, ofreciendo protección a sus

derechos básicos, como el derecho del sujeto de ser informado con anterioridad de la recolección de sus datos personales, así como el acceso a los mismos, la rectificación, la cancelación y la facultad de restringirlos de acuerdo a su voluntad.

2.4. El derecho a la intimidad

El derecho fundamental a la intimidad se encuentra consignado en el artículo 15 de la Constitución Nacional y se respalda en la Declaración Universal de los Derechos del Hombre, en el entendido de que todo individuo tiene derecho de reservar para sí, la información relativa a su particularidad y de decidir sobre a quién o quienes desea dar esa información y en qué condiciones, este derecho está expuesto a múltiples vulneraciones debido a intereses diversos, entre los que se cuentan los diferentes usos comerciales y la ventaja competitiva que representa tener la información de contacto de diferentes poblaciones de acuerdo al target de mercado de las mismas, así como la constante exposición en redes, internet y en general en el nuevo espacio tecnológico **(Alvarez, 2015)**.

Por ello, es necesario revisar el riesgo que presenta el derecho fundamental a la intimidad, cuando se exponen los datos personales, en pleno auge de la innovación tecnológica y el uso cotidiano que actualmente se le da en todo tipo de ámbitos, por lo tanto debe considerarse bajo una protección especial, teniendo presente que se encuentran inmersos los caracteres íntimos del desarrollo personal y la singularidad como ser humano.

En efecto, la exposición que se señala en lo que antecede, tiene que ver con la homogenización del colectivo y con el desconocimiento frente al tratamiento de los datos que se entregan todos los días distorsionados en tramites meramente transaccionales y/o de servicios

(Alvarez, 2015), en donde la autorización del uso de la información personal, desconoce la importancia de dicho manejo y las consecuencias que puede acarrear el uso discrecional de los datos.

Conforme lo anterior, se evidencia que hay un desconocimiento frente al límite de la información que se suministra dentro de una transacción o cuando se presta un servicio, pues se incluyen datos que en algunos casos no son relevantes para trámite **(Remolina Angarita, 2013)**.

Es entonces, cuando se vulnera el derecho a la intimidad, dado que el contenido de la información no es necesario para la transacción, de la mano de la vulneración del principio de libertad, toda vez que dicha autorización se termina convirtiendo en una aceptación tácita, información que a su vez es replicada por terceros no autorizados de manera concreta.

Como consecuencia, se presenta extralimitación en el uso de los datos personales suministrados, lo que termina desviando su finalidad inicial, no solo atribuyéndole esta falla al titular del dato, sino que a su vez puede conllevar a que se efectúen transacciones ilícitas, como se evidencia en los casos de suplantación de identidad.

Conforme lo anterior, se considera que si bien es cierto el habeas data señala la facultad de conocer, actualizar y rectificar los datos, también lo es que no se garantiza la efectividad de la protección del mismo, por cuanto se debería establecer un límite de uso desde el momento de la autorización **(Camargo, 2015)**.

Conforme lo anterior, debería indicarse un tiempo limitado de tratamiento, que tendría que corresponder al tiempo de concreción de la transacción, garantizando así, la eliminación o baja de la información al concluir el tramite transaccional correspondiente, lo cual esta vulnerado el

principio de temporalidad señalado en la Ley estatutaria 1266 del 31 de diciembre de 2008 que entre otros, así como los principios de finalidad, circulación restringida.

En resumen, el individuo estaría ejerciendo su derecho a la intimidad en el sentido estricto y original, al poder decidir qué parte de su información personal debe ser utilizada por otros y para que fines específicos.

2.5.La autorización del uso de datos personales

Como se ha evidenciado con anterioridad, el derecho a la intimidad y el derecho a la información, salvaguardados por la constitución nacional **(Congreso de la República, 1991)** se convierten de acuerdo al contexto globalizado en temas sensibles, dada la multiplicidad de riesgos a los que se expone.

Por tratarse de derechos fundamentales es necesario, entonces, darle prioridad a su protección y tomar las medidas necesarias para amparar y velar por el correcto funcionamiento del uso de los datos personales, así la autorización de datos personales debería hacerse de acuerdo con parámetros específicos en la legislación, con el fin de obtener mejores resultados en la prevención o en la sanción de las injerencias indebidas.

Es importante señalar , que el habeas data surge, como resultado de la necesidad de tener un derecho autónomo **(Camargo, 2015)** que permita conocer, actualizar y rectificar la información, que, en el caso de la primera ley relacionada con el tema de estudio, la Ley 1266 de 2008 **(Congreso de la República, 2008)**, inicialmente aplicada para la información financiera, es decir los datos referidos a los antecedentes financieros y vida crediticia del individuo.

Más adelante, dada la necesidad de cubrir otros ámbitos en la aplicación de la protección de los datos personales, en un sentido más amplio, se expide la Ley 1581 del 2012 **(Congreso de la República, 2012)** por la cual se dictan disposiciones generales para la protección de datos personales, que a su vez es reglamentada por el Decreto 1377 del 27 de junio de 2013 **(Congreso de La República, 2013)**.

Siendo esta última de carácter general enmarcando todos los ámbitos de recolección de datos personales sin que estos fueran ya únicamente de índole financiero.

Las disposiciones en materia legal, según la Ley 1581 de 2012 **(Congreso de la República, 2012)**, implican la autorización del uso de datos personales según la naturaleza de los datos, aquí, se reiteran los momentos en los que los ciudadanos ejercen su derecho, al conocer, actualizar y rectificar toda la información personal que se recopile o almacene, por parte de entidades públicas o empresas privadas.

En dicha ley **(Congreso de la República, 2012)**, además se dictan las disposiciones sobre las obligaciones que tendrán las entidades que tratan o manipulan los datos personales, entre los que se destaca la necesidad de que el titular de la información, autorice su uso y conozca con certeza la finalidad que tendrán dichos datos.

Así, la autorización del uso de datos personales es reiterada de formas distintas en la normatividad materia de este estudio, lo cual evidencia la pertinencia de generar mecanismos más eficaces de seguimiento y control en cuanto a la debida forma de hacerlo y de ampliar el conocimiento del individuo sobre el tema, en aras de una protección más amplia y efectiva en cuanto a la protección de datos personales y el derecho fundamental a la intimidad y a la información, señaladas inicialmente.

2.5.1. El consentimiento previo, expreso e informado del titular.

El titular de la información en cualquier caso, según Saldaña debe ser informado con anticipación de cuál será el uso que se le brindara a sus datos personales, no importa cuál sea el estamento que reciba los datos, el sujeto tiene el derecho de saber de forma clara y específica sobre el propósito de la recolección de los mismos y a quienes llegara la información. **(Nieves Saldaña, 2011**)

Así, debe existir la manifestación expresa de la ley, al señalar la prioridad de que el titular de la información almacenada exprese de forma clara su voluntad y conocimiento, en primer lugar, de entregar su información y en segundo, de entender el uso que tendrá.

Concretamente la Ley 1581 de 2012, en su artículo, 3 señala:

> *ARTÍCULO 3o. DEFINICIONES. Para los efectos de la presente ley, se entiende por:*
>
> *a) Autorización: Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales;"* **(Congreso de la República, 2012)**

En ese marco, también es importante traer al presente, el concepto de consentimiento mencionado por la Corte Constitucional en la Sentencia C-748 de 2011 **(Corte Constitucional, 2011)**, que habla sobre control de constitucionalidad del proyecto de ley estatutaria de habeas data y protección de datos personales, en la que se indica que existen tres etapas dentro del consentimiento calificado, refiriéndose expresamente a que este debe ser previo, expreso e informado.

Cuando habla de consentimiento en el sentido de su deber ser calificado, indica que debe ser previo, es decir debe realizarse en una etapa anterior a la incorporación del dato, en el momento

que el individuo decide poner sus datos en custodia y tratamiento de un tercero **(Corte Constitucional, 2011)**, llámese entidad pública o empresa privada.

Es importante generar una etapa previa, en donde se informe al ciudadano cuáles serán los parámetros bajo los cuales estarán protegidos los datos personales que está suministrando y de este modo, conocer y entender el tratamiento que se le dará al dato, es decir quienes tendrán acceso a dicha información y con qué fin, de tal manera, que sea posible dar inicio a la restricción previamente, para de este modo, conseguir por un lado cubrir de forma efectiva los derechos del individuo y de otro lado delimitar y evitar el uso indebido de la información que se esa suministrando.

Así mismo, cuando se habla de su condición de expreso, quiere decir que la información o los datos suministrados son verídicos **(Corte Constitucional, 2011)**, lo que indica la protección del dato para quien lo está suministrando, que debe garantizar que su información no sea tratada con fines diferentes a los establecidos inicialmente.

Para finalizar, frente a su naturaleza de ser informado, esto implica, que debe conocer la finalidad del tratamiento del dato suministrado **(Corte Constitucional, 2011)**, con el fin de restringir el mismo, por lo tanto es en esta etapa donde el proveedor o comerciante debe informar concretamente cual será el tratamiento que se dará a la información, y de este modo evitar la réplica de los datos a terceros no autorizados, convirtiendo los datos personales en una información de uso público sin ningún tipo de garantía a la reserva.

2.6. Aviso de privacidad y políticas de tratamiento de información

Para facilitar la puesta en marcha de la Ley 1581 de 2012, La Superintendencia de Industria y Comercio de ahora en adelante (SIC), tiene establecida entre otras La cartilla formatos modelo para el cumplimiento de obligaciones establecidas en la Ley 1581 de 2012 y sus decretos reglamentarios, en donde indica las políticas de tratamiento de información, orientando a los responsables y encargados del tratamiento de datos personales, respecto al manejo de la información, sugiriendo unos formatos a utilizar conforme las necesidades de cada caso..

Se entendería que con esta orientación brindada por la SIC, los responsables y encargados del tratamiento de datos personales implementarían alguna de las opciones que indica el ente de control en la cartilla, sin embargo, se evidencia que no se encuentra del todo establecida la obligatoriedad en algunas de las sugerencias establecidas en la misma, por cuanto se entienden como actividades opciones y no de estricto cumplimiento.

Conforme lo anterior, se evidencia que al no informar de manera concreta al titular del datos respecto del aviso de privacidad, se considera escasa la restricción de información que señala la ley **(Superintendencia de Industria y Comercio, 2017)**.

En este sentido, se concluye que esta medida no ha sido suficiente, por cuanto no se ha dado cabal cumplimiento a la normatividad ni a las sugerencias de la cartilla, de tal manera que entre otras el titular del dato desconoce la utilidad de su información o si será objeto de réplica, por tanto, debe considerarse la implementación obligatoria de un formato donde el titular pueda escoger a quienes desea que sea remitido su dato personal y el uso del mismo, basado en la protección del derecho fundamental a la intimidad. .

Lo que encontramos actualmente, en muchos de los casos en los que por diferentes motivos es necesaria la recolección de datos personales, es que las políticas de tratamiento de datos no son lo suficientemente específicas, abriendo la posibilidad del uso indiscriminado de estos y vulnerando ampliamente derechos fundamentales, como el de la intimidad **(Piñar Mañas, 2006)**.

Conforme lo anterior, se considera necesario establecer la obligatoriedad de implementación de formatos con datos específicos conforme la actividad a adelantar lo que conllevaría a indicar concretamente que tratamiento quiere que se le aplique a la información o dato personal.

Se evidencia entonces, que no existe en este momento la forma de asegurar al titular de la información, la destinación final de sus datos personales, de tal manera que se desconocerá las instancias a la cuales llegará o cuantas personas accederán a su información personal, lo cual hace imperativa la creación de mecanismos adecuados de prevención y sanción jurídica, evitando el uso indebido de la información personal y privada.

3. Capítulo 2: Marco Constitucional y Normativo de la gestión de la seguridad de la información de Datos personales

3.1.Disposiciones de la constitución colombiana sobre la protección de datos personales.

El uso de los datos personales se ha tornado indispensable, en todos los aspectos que tienen que ver con las relaciones sociales, económicas y políticas del contexto globalizado, tan es así, que se generó la necesidad de idear políticas públicas de origen supranacional sobre la recolección y tratamiento de datos, lo que hoy en día está consignado, entre otros, en la Declaración de los Derechos del Hombre, el pacto de San José o la Declaración Americana de Derechos y Deberes del hombre, allí se le otorgo atención especial a la privacidad y a la información personal, la cual hace parte de su vida privada.

Como resultado, muchos de los países vinculados a dichos organismos, adoptaron medidas en su legislación para la protección de la privacidad y el tratamiento de los datos personales, en Colombia la Constitución Nacional de 1991, le dio gran importancia a su protección estableciendo la salvaguarda de derechos fundamentales, como los referentes a la intimidad y el buen nombre (**Congreso de la República, 1991**).

Según Nelson Remolina (**Remolina Angarita, 2013**) este tema fue analizado de forma minuciosa en la asamblea nacional constituyente, donde generó varios análisis y debates, con el fin de no vulnerar ni poner en riesgo los datos personales o la intimidad de los ciudadanos, cuando las empresas privadas o públicas hicieran manejo de los mismos.

3.2.**Antecedentes y derecho jurisprudencial previo a Ley 1266 de 2008.**

La protección de los datos personales, no surge como necesidad a partir de un análisis precavido de una concepción ideológica o del estado, tampoco a partir de una necesidad política, su crecimiento, como ya lo he mencionado con anterioridad, es insipiente frente a una cotidianidad cada vez más bombardeada por la tecnología, la necesidad de protección ante este derecho, surge a partir de las nuevas formas de vida y de la irrupción cada vez más avasallante de la sociedad de la información.

Juan Carlos Upegui hace referencia a ello, y lo menciona cuando afirma:

"Fue una necesidad pragmática para encausar la defensa de valores ya clásicos y pacíficamente aceptados, como la libertad, la intimidad y la igualdad (**Upegui Mejia, 2008**)*"* Esto implicaba que su desarrollo, estaba ligado a comportamientos empresariales y de organizaciones, y que surgía con algunas confusiones jurídicas que deberían ser retomadas y formuladas en el desarrollo normativo futuro.

Posterior a la constitución de 1991 existieron varios pronunciamientos en sentencias, sobre lo que vendría en regulación para la seguridad en el tratamiento de datos personales, en 1992 la Sentencia T – 414, no tiene en cuenta el limite conceptual entre vida privada e intimidad y desarrolla una idea global de protección de la vida privada (**T - 414, 1992**).

Es en este primer antecedente cuando el derecho a la intimidad se empieza a vislumbrar como derecho madre, que brinda la posibilidad de agrupar un sin número de casos, además de servir de punto de partida al análisis normativo de temas como el secreto profesional, la imagen de las personas y el marco de tratamiento de datos personales.

En análisis jurisprudenciales posteriores se trataron algunos temas referidos también a la ambigüedad que suponía proteger el secreto y al mismo tiempo la libertad, basados en el

principio de bien común, lo cual según los magistrados presentaba una relación dicotómica o hasta contradictoria **(T - 022, 1993**).

La constitución del 1991 tiene como objeto generar las medidas necesarias para la pertinente recolección, manejo y tránsito de los datos de todos los individuos sin embargo, fue solo hasta el año 2002 que la Corte Constitucional, concreto los principios que darían validez y generarían los antecedentes de la ley de habeas data, en la sentencia T- 729.

Mediante esta sentencia, la corte, además, generó los tipos de datos personales, explicados en el capítulo que antecede y que tienen que ver con la información que es pública, la información semiprivada, la privada y por último la que es reservada (**T - 729, 2002**), que guarda una relación muy próxima, con los derechos fundamentales tales como la libertad, la intimidad, la dignidad o el buen nombre del titular de la información.

3.3.Marco Normativo general sobre la protección de datos personales, de Ley 1266 de 2008 o Ley de habeas data.

El primer acercamiento concreto a la protección de datos personales se obtuvo gracias a los antecedentes sugeridos anteriormente, la Corte Constitucional había clarificado y expuesto en varias ocasiones en sus sentencias, la necesidad de proteger los datos personales de las personas y con ello la salvaguarda de sus derechos fundamentales, como ser individual y como administrador de su información personal.

Con la ley de habeas data **(Congreso de la República, 2008)**, se promueve una protección especial a la información manejada en el sector financiero, es allí donde se explican los principios detallados con anterioridad y se establecen los marcos normativos en el tratamiento de datos de las entidades bancarias, crediticias, comerciales y de servicios.

Anteriormente en sentencia T – 440 de 2003, la corte había hecho concreciones interesantes sobre la reserva bancaria ligada al secreto profesional, y a que dicha reserva debe proteger los datos personales de la clientela **(T - 440 , 2003)**, cosa que generaría además credibilidad y confianza en los clientes de las entidades bancarias.

En la Ley 1266 de 2008, se establece el ámbito de aplicación, que será a la información personal registradas en bases de datos de entidades públicas y privadas, con excepción de las que pueden ser manipuladas con fines de seguridad nacional o internacional, como las manejadas por organismos como en su momento el Departamento Administrativo de Seguridad (DAS) o la fuerza pública.

Se establecen además en esta ley **(Congreso de la República, 2008)** , los principios de la administración de datos, mencionados anteriormente y se detalla la forma en la que puede circular la información personal, se estipula concretamente que pueden tener acceso a los datos; los titulares, los usuarios de la información, las entidades públicas que por su competencia los necesiten, los organismos de control que en el cumplimiento de sus obligaciones lo requieran y otras entidades cuyo objeto y finalidad sean de la misma naturaleza que la entidad que recopilo la información.

Finalmente especifica los derechos de los titulares de la información, frente a los administradores de bancos de datos, determina los deberes de los operadores de los datos y dicta las disposiciones frente a las peticiones, consultas y reclamos que podrán dirigir los individuos, al ver vulnerados de alguna manera sus derechos en cuanto a datos personales.

Evidentemente la ley que nos ocupa, contenía falencias, pues hasta ese momento se había pasado por alto, la necesidad de expedir una legislación diferenciada que tuviese como fin, la

protección de los datos personales que estuviesen por fuera del ámbito de aplicación, además de que la misma no restringía lo suficiente el destino y la forma de administrar la información de los operadores encargados.

Posterior a ello la Corte Constitucional expresa en el año 2008 que la ley de habeas data, trata la problemática de protección de datos personales solo de una manera parcial en sentencia C-1011, en donde concretamente dice:

"las consideraciones expuestas demuestran que el proyecto de ley tiene un propósito univoco, dirigido a establecer las reglas para administración de datos de contenido financiero y crediticio; […] no puede considerarse como un régimen que regule, en su integridad, el derecho al habeas data; **(C - 1011, 2008)***…"*

El principal propósito del derecho de habeas data según José Miguel de la Calle, es la posibilidad de participación activa del titular de los datos, en el tratamiento y administración de los mismos, con presencia y control de instituciones que tengan la idoneidad y pertinencia para ejercer veeduría efectiva del proceso **(De la Calle Restrepo, 2008)**.

Este derecho no se desliga o no depende de ningún otro derecho, es individual, independiente, por tanto, debe garantizarse sin condicionamiento a la intimidad, a la libertad personal o el buen nombre y la legislación debe estar en capacidad de proteger este derecho independientemente de los mencionados.

3.4. Ley 1581 de 2012

Para esta ley fue de vital importancia, la protección de la intimidad del individuo, la salvaguarda de sus características individuales personales y la tutela de su información más

personal, tal como lo advirtió en su momento la Corte Constitucional en sentencia T – 414 de ese mismo año:

"el núcleo esencial del derecho a la intimidad, supone la existencia y goce de una órbita reservada en cada persona, exenta del poder de intervención del Estado o de las intromisiones arbitrarias de la sociedad, que le permita a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural"

Los rasgos más sobresalientes de esta norma diferencial para la protección de datos personales **(Congreso de la República, 2012)**, son, entre otros, la definición de los principios de protección de los datos personales de; legalidad, finalidad, libertad, veracidad, transparencia y los más importantes, que hacen referencia a el principio de acceso y circulación restringida, confidencialidad y seguridad.

Se adiciona la facultad que tendrá el titular de autorizar previamente el uso y destinación de sus datos personales, los derechos del titular de la información, así como el deber del administrador de los datos, de informar el tratamiento al cual será sometida dicha información.

Por último, se esclarecen las condiciones de la consulta del titular o sus causahabientes y se prevé la forma de hacer los reclamos a que haya lugar, de no darse las condiciones previstas en la normativa.

En esta ley se tuvieron en cuenta, las necesidades identificadas por el legislador en materia de protección de derechos fundamentales como el habeas data, el buen nombre y la intimidad, el doctrinante Nelson Remolina **(Remolina Angarita, 2013)**, se refirió a la misma, afirmando que

se trata de una ley para exigir el adecuado tratamiento de la información individual de forma que no se vulneren sus derechos y libertades.

En el caso de la Ley 1581 de 2012, la protección se presenta frente a cualquier base de datos sin distinción, no solo frente a entidades bancarias, crediticias o comerciales, como en la normativa vista anteriormente, lo que obligó a entidades de todos los ámbitos, bien fuesen públicas o privadas a replantear el manejo de la información personal que se encontraban en sus registros, hacer un manual de políticas de datos donde se especificara la procedencia y destinación de los datos personales y contar con registros de consulta en donde los titulares de la información pudiesen verificar lo anterior.

Dicho de otro modo, esta normativa prevé que los datos deben ser recolectados únicamente para la destinación prevista y que esta, debe ser legitima y explicita, que los administradores de base de datos no pueden excederse en cuanto a lo absolutamente necesario para el fin enunciado, además de que deben ser pertinentes y adecuados y en definitiva deben estar en disposición para consulta del titular de la información, de forma permanente **(Congreso de la República, 2012)**.

Hay un procedimiento especial en cuanto a los datos sensibles o los que afectan o vulneran la intimidad de los sujetos o cuyo uso indiscriminado puede dar lugar a exclusiones de carácter racial, política, filosófica etc., así mismo exige un trato diferencial con el manejo de datos de los niños, en concordancia con la protección especial que estos revisten.

Es pertinente generar un análisis que vaya más allá de los usos ilegales o con fines delictivos, que permita precisar, que el uso indiscriminado de los datos por parte de los administradores de las bases puede generar una vulneración a los derechos fundamentales del individuo, toda vez que el administrador, aún tiene facultad para tomar decisiones que afectan de

forma negativa al ciudadano, con desconocimiento preciso sobre ello, también pueden elaborarse además perfiles incorrectos o que sugieran una información desacertada o que no ha sido aportada por el titular de la información.

La afectación podría también darse en términos más sencillos, por negligencia de los administradores de los datos, cuando este no actualiza o renueva los mismos o cuando no toma las medidas de seguridad necesarias para que los mismos no sean obtenidos por terceros, con intereses distintos a los de la recolección de la información.

Lo anterior supone que es necesaria una legislación que tenga en cuenta estos casos, que efectivice de forma acertada la protección de los datos personales, que brinde verdaderas garantías a los titulares de los datos y que asegure unas sanciones apropiadas para los administradores de datos que incurran en este tipo de negligencia.

3.5. Control de Constitucionalidad Ley 1581 de 2012.

La revisión de pertinencia con la norma constitucional, determino que en términos generales la ley que nos ocupa cumplió con los requisitos constitucionales, existiendo unidad de materia y concordancia con lo establecido, sin embargo, se presentan algunas dudas en lo referente a la forma o disparidad entre la norma y los derechos fundamentales, pues las corte, en este caso revisa que sean coherentes con su núcleo esencial, todo lo adyacente, como la consagración de limites o restricciones, son potestad del legislador.

El tramite seguido en la cámara, que inicio en la comisión primera cumplió a cabalidad los requisitos de debate y fue aprobada por la cámara de representantes y el senado, en votación nominal, por mayoría absoluta.

Se vieron afectados los principios de consecutividad e identidad relativa dado que algunos artículos (manejo de datos judiciales y tratamiento de datos personales por parte de inteligencia y contrainteligencia) fueron incluidos de forma improvisada, sin que surtieran los requisitos necesarios en cuanto al análisis y discusión de los mismos, al no presentarse los debates reglamentarios.

Dentro de los contenidos mínimos, que debería tener la reglamentación sobre datos personales se contemplaron; el derecho del titular de la información a conocer y tener acceso a lo consignado por ellos en bases de datos, el derecho a retroalimentar y actualizar los datos consignados, así como el derecho a corregir la información o excluir una parte de ella de acuerdo a su criterio.

3.6. Reglamentación: Decreto 1377 de 2013

Para la correcta aplicación de la ley descrita en lo que antecede, se determinó que tendría que ser complementada y se expidió el Decreto 1377 en el año 2013, cuyo objetivo sería reglamentar efectivamente, temas relacionados con la política de tratamiento de datos que debería desarrollar el o los responsables del manejo de información personal, la autorización del uso de la misma y la pertinencia de la cantidad de datos suministrados respecto al fin destinado para ello **(Congreso de La República, 2013)**.

De este modo este decreto, fortalece lo determinado por la Ley 1581 de 2013, toda vez que incorpora una descripción explicita de los procedimientos usados, para la recolección, circulación, manejo y eliminación de los datos personales suministrados por el titular, además de

limitar el tiempo en el que los mismos estarán a disposición del administrador de la base de datos, al estrictamente necesario.

Sin embargo, a pesar de los esfuerzos de los legisladores en materia de protección de datos personales, aún existen vacíos en la norma, principalmente en cuanto a la circulación, que si bien debe ser informada al titular de la información **(De la Calle Restrepo, 2008)**, puede también ser direccionada a terceros que tengan el mismo objeto de la entidad pública o privada que los recolecta, toda vez que no se guarda una adecuada trazabilidad de los mismos y su destinación final, en este orden de ideas puede llegar a ser desconocida.

3.7. Principios de la protección de datos personales

En la sentencia enunciada al principio de este capítulo, **(T - 729, 2008)**, se enuncian por primera vez los límites que tendrá en adelante el tratamiento de datos personales, los cuales guardan carácter vinculante y un carácter práctico a la hora de establecer deberes específicos y concretos sobre ideas fundamentales indispensables para la protección de la información de carácter individual.

Por otro lado, son los principios en materia de protección y gestión de la seguridad de datos personales los que determinan si el manejo de la información se está realizando dentro de los parámetros legales, adecuados y transparentes según lo conceptuado por Nelson Remolina **(Remolina Angarita, 2013)**.

Esos principios mínimos de la protección de datos personales en Colombia (), comprenden:

1.” Principio de libertad, entendido como aquella autorización previa, libre y expresa del titular de la información que se confiere para su registro y su divulgación, concretándose así una ilicitud la obtención de la misma sin esta autorización.

2. Principio de necesidad, como aquel que hace alusión que serán registrados aquellos datos que se hagan estrictamente necesarios para el objeto perseguido con su obtención, concretándose así que no se puede registrar o circular aquella información que no sea necesaria.

3. Principio de integridad, el cual va de la mano del principio de veracidad bajo el cual los datos personales deben ser registrados de manera completa, siendo así que el registro de información de datos parciales, incompletos o fraccionados se configura en una ilegalidad.

4. Principio de finalidad, la recolección, tratamiento y circulación del dato personal debe obedecer a un fin.

5. Principio de utilidad, el tratamiento y la circulación del dato personal deberá cumplir una función determinada.

6. principio de circulación restringida, ligado al principio de finalidad de la cual deviene que tanto la divulgación como circulación deberá tener límites específicos.

8. Principio de incorporación, opera cuando al titular de la información le conviene incluir información adicional a dichas bases de dato de tal manera que no se podrá negar su incorporación.

9. Principio de caducidad, la información que afecte al titular de la misma deberá ser retirada de las bases de datos obedeciendo a criterios de razonabilidad y oportunidad, de tal manera que la información no podrá estar contenida en bases de datos de manera indefinida.

10. Principio de individualidad, los datos personales deben ser almacenados de forma independiente para evitar así el cruce de datos.

11. Principio de diligencia en el manejo de los datos personales, el cual exige de los administradores de las bases de datos personales un comportamiento diligente, tendiente a cumplir con los postulados establecidos en la legislación para su protección.

12. Principio de la obligación de indemnizar los perjuicios causados por las posibles fallas en el proceso de administración, deviene cuando se presentan fallas en el proceso y se configuren los elementos generales de la responsabilidad civil, imponiéndosele la carga a titular de la información de demostrar que el daño sufrido fue a causa de la actuación del operador de los datos"

Los principios en materia de protección de datos son un instrumento de aplicación general que permiten poner un marco mínimo de responsabilidad frente al manejo y tratamiento de los mismos, por su carácter vinculante y constituyen una pieza fundamental sobre la correcta aplicación y la interpretación de lo legislado en la materia.

3.8.El papel de la Superintendencia de Industria y Comercio:

Esta entidad es la encargada de ejercer control y vigilancia en lo concerniente a la protección de bases de datos, maneja entre otras cosas la regulación sobre el registro de bases de datos y la delegatura de protección de datos personales.

En lo concerniente al registro nacional de bases de datos, en adelante RNBD, la superintendencia tiene a cargo el directorio público de este registro, los datos consignados allí, son los que están sujetos a tratamiento y son de fácil acceso y consulta para los ciudadanos, en el

decreto único referente al tema el 1074 **(Presidencia de la república, 2015)**, se reglamentó la información términos y condiciones que deberán acatar los administradores de las bases de datos.

El Decreto 090 del 18 de enero **(Presidencia de la República, 2018)**, determino la aplicación del RNBD y fijo los plazos en los cuales los administradores deben hacer la inscripción de bases de datos, que según lo dispuesto por esta reglamentación deben ser las entidades sin ánimo de lucro y las sociedades o empresas unipersonales públicas o privadas que tengan activos superiores a cien mil unidades de valor tributario (UVT).

Existen unos plazos establecidos para realizar el registro de las bases de datos: el primero de ellos es para las sociedades y entidades sin ánimo de lucro que tengan activos por más de 610.000 UVT, que deberían haber registrado sus bases de datos antes del 30 de septiembre de 2018.

En cuanto a la implementación del Principio de Responsabilidad Demostrada **(Superintendencia de Industria y Comercio, 2015)** (Accountability) referida a la puesta en marcha de acciones dentro de las organizaciones y/o entidades que tienen a su cargo la recolección de datos y su responsabilidad frente al trato adecuado de los mismos dando cumplimiento a los principios de privacidad y protección de datos, basados en las Guías sobre Protección de la Privacidad y los Flujos Transfronterizos de Información emitido por la OCDE de 2013, de tal manera que la Superintendencia de Industria y Comercio establece el marco desde el cual deben actuar los administradores de la información personal, en ese sentido, el ente de control ha expedido La Guía para la Implementación del Principio de Responsabilidad Demostrada en donde señala los fundamentos básicos para el desarrollo de un programa integral de gestión de datos personales **(Superintendencia de Industria y Comercio, 2015)**, basado en la reglamentación otorgada en el Decreto 1377 de 2013.

En esta guía indica los aspectos más relevantes que debe desarrollar el administrador de datos personales para un adecuado manejo y promueve el compromiso de cada organización frente a la importancia de preservar la privacidad y en cuanto a las medidas pertinentes para la protección de los derechos de los usuarios.

De tal manera, es menester que los administradores y responsables de la información personal deben conocer a cabalidad los datos personales almacenan, haciendo un inventario continuo, que genere además una trazabilidad sobre su uso o su necesidad, propendiendo porque estos realmente sean útiles para la finalidad establecida por la empresa o corporación.

De otra parte, la Delegatura de la Superintendencia de Industria y Comercio es la autoridad en protección a datos personales, ella se encarga del cabal cumplimiento del marco legal y proponer nuevas disposiciones en la materia, también es el órgano encargado de emitir las circulares con las diferentes disposiciones, sanciones y requerimientos en materia de protección de datos.

3.9.Régimen sancionatorio

En la Ley 1581 de 2012 se determinó que el organismo encargado de ejercer la vigilancia y control sobre la protección de datos personales seria la Superintendencia de Industria y Comercio **(Congreso de la República, 2012)**, es ella la encargada de garantizar el manejo adecuado de la información de los ciudadanos, quien debe velar por el respeto de los derechos y garantías consignados en la ley, así como ejercer los procedimientos que establece la misma, en caso del incumplimiento de alguno de los parámetros establecidos.

Entre sus labores se encuentra el realizar las investigaciones pertinentes y efectuar medidas conducentes a la protección de los derechos del titular de los datos personales y de ser necesario

bloquear la información, si la investigación previa pertinente arroja vulneración de estos derechos, mientras se determina la responsabilidad del administrador de las bases de datos **(Superintendencia de Industria y Comercio, 2017)**.

Dentro de los deberes de esta superintendencia se encuentra, generar acciones preventivas, frente a los posibles riesgos por medio de campañas de divulgación e información para que los ciudadanos tengan el conocimiento sobre sus derechos como ciudadanos, al hacer entrega de sus datos personales a los diferentes organismos tanto públicos y privados.

Deben también emitir órdenes para el correcto funcionamiento de la administración del registro nacional público de bases de datos, proponer los aspectos de mejora necesarios, para el cumplimiento del marco legal y constitucional, además de solicitar la cooperación a nivel internacional cuando en la recolección de datos, los titulares observen alguna afectación.

En los casos de vulneración de la información del titular y el incumplimiento por parte de los administradores el ente de control tiene la facultad de imponer sanciones de acuerdo con la gravedad del hecho **(Superintendencia de Industria y Comercio, 2017)**, las sanciones de tipo económico van desde dos mil salarios mínimos mensuales vigentes infringidos a la persona natural o jurídica que haya cometido la vulneración, además podrá ordenar la suspensión de la recolección y manejo de datos hasta por seis meses, puede haber cierre temporal por incumplimiento a las sanciones de la superintendencia y clausura definitiva de tratamiento de datos sensibles.

Si bien la Superintendencia de Industria y Comercio intenta cumplir a cabalidad los requerimientos de los ciudadanos en cuanto a la protección de los datos personales, la falta de cobertura de la ley como en la calidad de los datos y la finalidad de los mismos, no permite

generar las sanciones efectivas, que aportarían a la disminución de la vulneración de derechos fundamentales como el referente a la intimidad, que está ligado a la integridad y dignidad del hombre.

Además, el desconocimiento de la población hacia sus derechos como titular de sus datos personales, no permite que comuniquen y/o acudan al organismo de control frente a las posibles vulneraciones de las que son víctimas en las operaciones cotidianas comerciales o de cualquier naturaleza.

A pesar de lo señalado en materia legislativa en lo referente a bases de datos, se ha encontrado que a pesar de lo previsto en la misma, la labor de protección de los derechos de habeas data ha estado a cargo de la Corte Constitucional por vía de la acción de tutela, lo que supone que la legislación actual no es suficiente y que posterior a la intervención de los administradores de bases de datos ha sido necesaria la acción judicial posterior (ex post facto), con miras a proteger los derechos fundamentales de intimidad o buen nombre.

Lo anterior evidencia, que son los administradores quienes deciden de forma autónoma el tiempo de permanencia de datos personales en las bases de datos, sobre todo en temas de información negativa sobre solvencia financiera y patrimonial, dando como resultado según el caso, un tratamiento discriminatorio, que tendrá consecuencias de exclusión y vulnerará de forma directa la intimidad del titular de la información.

4. Capítulo 3: buenas prácticas aplicables a la gestión de la seguridad de la información de Datos personales.

4.1.Buenas prácticas internacionales

Como se ha anotado con anterioridad, las primeras nociones frente a la gestión de la seguridad de datos personales se dieron en Europa, con la proclamación universal de los derechos humanos, allí empezó a darse importancia al hombre como ser individual sujeto de deberes y derechos, entre los cuales aparecía por primera vez, el referido a la intimidad personal.

A pesar de ello en ese ámbito solo eran reconocidos factores muy concretos de la intimidad, como los derechos de protección en cuanto a las comunicaciones, el carácter secreto y personal de la correspondencia y lo referido a la protección de domicilio, no se reconocía la intimidad como un derecho unitario **(Piñar Mañas, 2006)**.

Actualmente, sin embargo, los grandes avances tecnológicos, sumados a la efectividad de los procesos empresariales que han simplificado y dado celeridad y seguridad a las dinámicas sociales y administrativas, por lo cual se ha hecho necesaria la regulación en cuanto a recopilación de datos.

Así, la informática constituye hoy en todos los lugares del mundo, más que un medio, el poder que supone tener al alcance mucha información, lo que ha sido llamado la democratización de la información, dadas las condiciones de accesibilidad masiva a las redes informáticas, por ello es sin lugar a dudas un instrumento muy poderoso de recopilación de información **(Camargo, 2015)**.

La sociedad europea ha entendido entonces, que el poder ya no reside en la imposición de la fuerza física o la coerción mediante los métodos ordinarios, sino en la información personal con la cual es posible controlar los rasgos conductuales de los individuos, por ello, es tan importante

para la legislación europea proteger la información personal y generar medios efectivos para su prevención y las sanciones a las que hay lugar en el momento que dicha información es transgredida o tratada de forma inadecuada.

La acepción de intimidad en su sentido amplio, procedente de la declaración de los derechos humanos y ha sido adoptada por la constitución de la mayoría de países europeos, ahora bien, dado el crecimiento tecnológico de los últimos años, los países también han reconocido nuevos mecanismos de protección que se centran en la supervisión del trámite adecuado de datos personales en el nuevo contexto informático vanguardista **(Alvarez, 2015)**.

En Europa, los países pioneros son España, Alemania y Portugal, quienes han consignado y generado mecanismos de protección en su marco constitucional y normativo, en lo que respecta a protección de información personal. A continuación, se realizará una recopilación y análisis de las buenas prácticas en el continente europeo.

4.2. Buenas prácticas europeas

La comisión consultiva que estudiaba las nuevas tecnologías y su impacto en la normatividad y los derechos de los ciudadanos fue creada por el consejo de Europa en el año de 1967, gracias a ello en el año inmediatamente posterior se creó la resolución que versaba sobre la relación de los nuevos estudios científicos y tecnológicos y los derechos fundamentales del hombre, **(Resolución 509 , 1968)**, que más tarde se convertiría en la resolución de protección de datos.

A partir de allí, la protección de datos personales se ha hecho presente en la normatividad europea, en algunos casos de forma tácita, pero en la mayoría su desarrollo se ha consignado de forma expresa, de acuerdo a la importancia que le han otorgado este continente a la protección de la información en medio de la masividad que hoy en día representan los grandes avances tecnológicos.

En lo que sigue revisaremos algunos casos específicos.

4.2.1. Buenas prácticas en la normatividad española

El orden constitucional español, integra dentro del apartado que trata los derechos fundamentales lo siguiente:

"*la ley limitara el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos*" **(Constitución Española, 1978)**

Más adelante en el mismo articulado, la constitución española se refiere a la regulación que deberá ejercer la ley respecto al acceso a los archivos y todo tipo de registros de índole administrativa, exceptuando lo relativo a seguridad y defensa del estado, la intimidad de titular o la información de su pasado penal judicial.

Lo anterior se contrapone un poco con el articulo 20.1 literal d) que se refiere al derecho básico de obtener información, sin embargo, en este se hace énfasis, en que será ejercido teniendo en cuenta que el límite del mismo es la intimidad personal **(Constitución Española, 1978)**, de esta forma la intimidad se antepone a el derecho a informarse, lo cual genera una nueva perspectiva en donde la intimidad no solo se opone a las intromisiones al espacio personal, sino que además agrega la facultad de poder controlar la información que reciben otras personas.

Las últimas reformas han pretendido dirigir esta reglamentación también para los casos informáticos, tal es el caso del artículo 18.4 que de forma expresa señala un límite al uso de la informática, para garantizar la intimidad individual y familiar, lo cual en su sentido más amplio protege el uso general de los derechos ciudadanos, de lo que se infiere que su interpretación se haga en un sentido progresivo.

Por otro lado, su interpretación en la protección de lo colectivo se manifiesta en el artículo 10.1 que menciona el libre desarrollo de la personalidad y de la dignidad humana, constituyéndolo literalmente como la base de la paz social y el orden político establecido en la república española.

Esta legislación otorga a los poderes públicos, la obligación de velar por la efectividad de la libertad y la igualdad del individuo, quienes además deberán apartar los impedimentos que dificulten dicho propósito promoviendo la participación de las personas en la sociedad y en la vida política, económica y cultural del país **(Parlamento Europeo, 1995)**.

Este desarrollo normativo, que incluye como derecho fundamental expreso la protección de datos personales, ha facilitado el control de todos los aspectos que rodean la recolección y administración de la información, incluyendo los que tienen que ver con la informática y las nuevas tecnologías, cubriendo de forma particular este importante ámbito del ciudadano español.

4.2.2. Buenas practica en la normatividad alemana

Alemania sigue la tendencia de los países europeos, fundamentando su preocupación en la protección del ciudadano, ante los riesgos que representa la cada vez más creciente revolución informática, lo cual tiene como base que:

"la ley fundamental es un ordenamiento comprometido con valores, que reconoce la protección de la libertad y de la dignidad humana como fin supremo de todo derecho **(Organizacion de Naciones Unidas, 1948)***"*

Esta ley le da gran importancia a la injerencia de la informática, sobre todo en lo relacionado con el estudio, reconocimiento del tratamiento de la información personal por parte de medios automatizados, así se evidencia en una ley alemana llamada Grundgesetz **(Boletin Oficial Federal, 1949)**, allí se le ha dado reconocimiento expreso a un derecho que han llamado autodeterminación informativa **(Rivera Llano, 2008)**.

En la constitución alemana no hay un reconocimiento al derecho de protección de datos, en ningún contexto, sin embargo, el alto tribunal alemán parte de la aceptación general de la libre personalidad de los individuos, lo cual construye en torno a la importancia de la dignidad humana y la libertad propiamente dicha.

Lo que sugiere que este derecho a la libre personalidad debe abarcar el respeto por la conciencia y la autodeterminación **(Remolina Angarita, 2013)**, en todos los campos en que esta intervenga, lo que implica que el ciudadano es capaz de pensar y actuar de acuerdo a sus convicciones con responsabilidad, teniendo la posibilidad de incidir sobre su entorno, en cuanto a cuál es la información que quiere que sea visible y publica y cual previere reservar.

Los riesgos de la ley en cuanto a la protección de la esfera privada tienen que ver con la transmisión de forma discrecional de los datos **(Camargo, 2015)**, sin conocimiento del titular de los mismos o que los datos que han sido almacenados, aun cuando sean verídicos, pueden ser dados a conocer fuera del contexto en el cual se recibieron, dando lugar a interpretaciones incorrectas.

En este caso la ley no menciona de forma concreta la defensa de este derecho, siendo la jurisprudencia del Tribunal Constitucional Alemán, la que ha dado forma y concretizado lo concerniente a protección de datos personales.

4.2.3. Buenas prácticas en la normatividad de Portugal

Portugal es una de las naciones que más ha puesto interés en la gestión de la protección de los datos personales, su constitución está enmarcada en la protección de los derechos fundamentales y en ella se expresa claramente en su apartado 37, 1er apartado:

"Todos los ciudadanos tendrán derecho a tomar conocimiento de lo que conste en forma de registros mecanográficos acerca de ellos y de la finalidad a que se destinan las informaciones y podrán exigir la rectificación de los datos, así como su actualización" **(Constitucion de la república portuguesa, 1976)**.

Este artículo integra de manera general los conflictos que puedan suscitarse entre la libertad de la informática y el derecho a la intimidad, lo cual no da cabida a ambigüedades, existiendo en esta última norma constitucional una mejor elaboración práctica y técnica.

Además, delinea muy bien las ocasiones en las cuales se podrá utilizar la informática para el tratamiento de datos personales **(Constitucion de la república portuguesa, 1976)**, dejando claro que no se usaran en casos de tendencias políticas, pensamiento religioso o en del círculo íntimo del individuo, a no ser que no sean identificables y sean usados únicamente para fines estadísticos.

Cuando el derecho de uso y tratamiento de datos personales se manifiesta de forma tan clara, como es el caso del derecho portugués, se presenta un cubrimiento mayor de la intimidad personal y se protege de forma más asertiva el derecho de autodeterminación informática y el buen nombre, permitiendo así mismo generar mayor control sobre el manejo de la información de los ciudadanos.

Tabla 1 Cuadro resumen de principales aportes de buenas prácticas europeas

País	Leyes sobre protección de datos.	Principales aportes
España	Constitución española 1978	-Establece límites sobre el uso de la informática, con el fin de proteger la intimidad y privacidad de las personas. -Regula todo tipo de acceso a archivos administrativos y de toda índole. -Tiene un lugar explícito en la constitución. -Garantiza la intimidad individual y familiar.
Alemania	Ley fundamental Grundgesetz 1949	-Concede especial importancia a la informática en el tratamiento de la información personal, cuidando los límites para que no vulnere el derecho a la intimidad. -Autodeterminación informativa. -Preponderancia del libre desarrollo de la personalidad, las libertades individuales y la Dignidad del ser humano.
Portugal	Constitución de la República portuguesa 1976	-Se enuncia en la norma constitucional como derecho fundamental.

	-Regulariza y Clarifica los límites de la informática frente a la intimidad del individuo y frente al adecuado tratamiento de los datos personales.

Tabla No 1: Elaboración Propia en base a referencia bibliográfica.

4.2.4. Generalidades y Análisis de buenas prácticas europeas

La labor en la construcción doctrinal, jurisprudencial y normativa de los países europeos ha marcado la necesidad para otros países de incluir la problemática que traen consigo las nuevas tecnologías **(Prado, 2012)**, en cuanto a la inferencia de estas en la vida diaria del individuo, tan es así que ha prevalecido, frente a intereses comerciales, como es el caso de las redes sociales, y lo ha conseguido precisamente, porque en la mayoría de los casos se expresa de forma textual, sin dejar dudas a ambigüedades jurídicas.

Hemos reconocido a lo largo de este capítulo, tres factores importantes que aportan a las buenas prácticas por parte de las naciones europeas: en primer lugar, la claridad del derecho portugués en cuanto a la elaboración constitucional referente a la protección de datos y el marco en el cual debe darse su vínculo con la informática, que no deja dudas del proceder.

En segundo lugar se evidencia el trabajo doctrinal y jurisprudencial de la republica alemana, que incluye el concepto de autodeterminación informática **(De la Calle Restrepo, 2008)**, que facilita la interpretación de la norma referente a protección de datos personales, además de delegar parte de la responsabilidad en el ciudadano, en cuanto al uso de su información privada, al hacer parte de una sociedad libre.

Y por último la construcción jurídica en España, que integra el derecho fundamental a la protección de datos, reconociendo su tratamiento en un marco concreto y especificando como limite el derecho a la intimidad, lo que genera, como en el caso portugués, mayor claridad en cuanto a su aplicación y régimen sancionatorio.

Estos países han entendido que la normatividad debe construirse teniendo en cuenta el contexto y que, dadas las actuales circunstancias de avance tecnológico, deben crearse nuevos escenarios jurídicos que salvaguarden el ámbito privado y de intimidad de las personas.

En relación a Latinoamérica, como se verá a continuación la normativa europea, lleva mucha ventaja, no solo en lo que se ha anunciado con respecto a la posible injerencia de la tecnología en la vulneración del derecho a la intimidad y a la privacidad, tanto individual como familiar, sino que además establece de forma general límites claros, en los eventos donde los derechos se ven afectados, así como las restricciones de los administradores de la información.

4.3.Buenas prácticas en Norte América

En estados unidos el derecho referente al tema que nos ocupa, está centrado en la privacidad, es allí donde la legislación ha puesto su mayor empeño, que si bien no se ha hecho de manera sistemática u homogénea, si se hace una especial mención alrededor de su protección **(Nieves Saldaña, 2011)**, es así como la constitución estadunidense ha conceptualizado y generado contenidos respecto de la primera enmienda, como en el caso cuando libera al ciudadano de revelar su adhesión a grupos o asociaciones de talante ideológico, brinda garantías en los casos

de registro arbitrario y en el caso de la quinta enmienda cuando menciona el derecho a la no autoincriminación y la no obligación de aportar sus datos personales.

Una de las principales aportaciones al respecto, es el principio de la privacidad del Common Law Rigtht to Privacy **(Warren, 1980)** (Derecho común, derecho a la privacidad) , la cual influyo de forma importante en diversas áreas del derecho norteamericano e incidió considerablemente en el desarrollo normativo y jurisprudencial en torno al derecho a la privacidad, como se puede ver en lo que a intimidad personal y familiar se refiere **(Nieves Saldaña, 2011)**.

La necesidad de legislar en tal sentido, se da a raíz de la aparición de nuevas y cada vez más invasivas tecnologías, por ello los legisladores americanos conceptualizan lo que se llamara Common Law Rigtht to Privacy **(Warren, 1980)** , que implica la oportunidad para el individuo de escoger que parte de su información personal quiere que sea expuesta, para que fines y en qué condiciones y limita el uso abusivo de tecnologías en medios de comunicación, desarrollando, entonces el derecho a no ser molestado respecto al círculo íntimo y generando la libertad de divulgar solo parte de la información.

La legislación que proponía el derecho a la privacidad tuvo poca asimilación al comienzo, tuvo un largo proceso de ajuste que estuvo ayudado por las múltiples alusiones en materia de jurisprudencia **(Prado, 2012)**, sobre todo en los principales tribunales de New York, a partir de los años sesenta, dado el contexto de libertad personal y de conciencia que se daba en el contexto.

4.4.Buenas prácticas en América Latina

En América latina estos procesos se han dado de forma más tardía y a pesar de la influencia de Europa, Estados Unidos y los tratados internacionales firmados por países de la región, han sido pocos los que han logrado incluir en su normatividad, de forma clara la protección de datos personales, de hecho, la mayoría no lo reconocen en su norma constitucional como un derecho fundamental.

Las nuevas tecnologías han entrado también con fuerza al ámbito latinoamericano, la democratización del internet ha llevado a que cada vez más personas en esta región tengan acceso a un sin número de información que no se encuentra controlada, ni registrada **(CEPAL, 2010)**, solo algunos países han previsto algunos de los riesgos que reviste la no protección de la información personal.

4.4.1. Buenas prácticas en Argentina

Argentina es uno de los pocos países en América latina que ha adoptado algunos de los preceptos europeos, así se evidencia en el artículo 43 de la constitución en donde hace referencia expresamente a ello, después de la reforma hecha en el año de 1994:

"*Toda persona podrá interponer acción para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquellos* **(Constitucion de la Nacion Argentina, 1853)***"*

Existe además una normativa sobre protección de datos que trata sobre las disposiciones generales en la materia **(Ley 25.326, 2000)**, así como una específicamente para la ciudad autónoma de Buenos Aires **(Ley 1845 de Proteccion de Datos., 2006)**, esta legislación es según varios doctrinantes, una de las mejores, dado que acoge lo mejor de la normatividad europea al sistema normativo latinoamericano, relacionando expresamente en su columna vertebral, el derecho fundamental que subyace del derecho y la protección de la intimidad.

El problema de esta y muchas de las legislaciones latinoamericanas, es que se tiende a mezclar los conceptos, es necesario hacer una distinción más elaborada entre lo que denominan intimidad, honor, buen nombre o protección de datos personales.

4.4.2. Buenas prácticas en Uruguay

En la constitución uruguaya no se hace mención de forma expresa de la protección de los datos personales, solo se realizan acercamientos generales como el que reza en el artículo 28:

"Los papeles de los particulares y su correspondencia epistolar, telegráfica o de cualquier otra especie, son inviolables **(Constitución de la República Oriental del Uruguay, 1967)***"*

Sin embargo, esta legislación también está inspirada en la legislación europea, toda vez que cuenta con una ley específica de protección de datos y habeas data **(Ley 18.331 , 2008)** en donde llama la atención primordialmente que el titular del dato puede ser una persona jurídica, por lo demás sigue muy de cerca los lineamientos de la normatividad argentina, poniendo como principal foco de protección la intimidad de las personas.

Esta además, el Decreto 414 **(Decreto 414, 2009)**, que reglamenta la ley que antecede, en donde se evidencia un trato más severo para los que infrinjan la ley, pues el régimen sancionatorio habla de 500mil pesos uruguayos, es decir hasta 43 millones de pesos colombianos, lo que a todas luces puede evitar de forma efectiva la violación de la norma.

4.4.3. Buenas prácticas en Perú

Su constitución en el artículo 2 inciso 5 determina:

"Toda persona tiene derecho a solicitar sin expresión de causa la información que requiera y a recibirla de cualquier entidad pública, en el plazo legal (……). Se exceptúan las informaciones que afectan la intimidad personal y las que expresamente se excluyan por ley o por razones de seguridad nacional **(Constitución Nacional del Perú, 1993)***"*

Es así mismo se evidencia la ley de Protección de Datos Personales Ley No. 29733, de 3 de julio de 2011 **(Congreso de la República, 2011)**, en la cual enmarca un régimen sancionatorio conformado en infracciones y sanciones cuya clasificación va desde muy graves, pasando por graves y leves, su sanción económica también es alta y su atención principal está dirigida a la protección de la intimidad.

Los derechos, con los que cuenta el ciudadano sujeto de los datos personales, son más amplios y comprenden: Acceso, actualización, inclusión, rectificación y supresión, impedimento del suministro, oposición, tratamiento objetivo y tutela **(CEPAL, 2010)**, lo cual de alguna manera brinda una protección más efectiva, pues cubre de manera más específica, las posibles violaciones a la norma.

Además de estos rasgos la legislación peruana ha previsto la injerencia de la informática en la privacidad de las personas y en busca de mitigar esta intromisión ha expuesto textualmente su preocupación en la constitución:

"Toda persona tiene derecho... A que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar **(Constitución Nacional del Perú, 1993)***"*.

Perú y Venezuela son los dos únicos países de Latinoamérica que han manifestado su preocupación en cuanto a la injerencia de las nuevas tecnologías en la intimidad y el círculo íntimo de las personas **(Prado, 2012)**, siendo estos los que llevan la delantera en cuanto a la reglamentación para impedir la utilización de la tecnología como factor de interrupción de derechos tales como la intimidad, el buen nombre o más aun como detonante de procesos de exclusión entre los ciudadanos.

4.4.4. Buenas prácticas en Venezuela

Como se indicó con anterioridad, Venezuela explora la posibilidad de que las nuevas tecnologías sean una amenaza inminente para la intimidad de las personas, de ese modo lo señala la constitución de este país que textualmente dice:

"Toda persona tiene derecho a la protección de su honor, vida privada, intimidad, propia imagen, confidencialidad y reputación. La ley limitará el uso de la informática **(Constitución de la Republica Bolivariana de Venezuela, 1999)**".

Tal como se dio en Europa, en Venezuela decidieron incluir la regulación de las nuevas tecnologías en el ámbito constitucional y normativo, enlazándolo directamente con el derecho a la intimidad.

El resto del articulado no trae grandes cambios con respecto a otras normatividades latinoamericanas, en la ley principal al respecto, la Ley Orgánica 15/1999 **(Jefatura del Estado, 1999)**, de Protección de Datos de Carácter Personal y el **(Parlamento Europeo, 2007)**, se destaca que el derecho a la intimidad ha presentado modificaciones significativas en el cuerpo normativo, que ha evolucionado de ser una libertad en sentido negativo, es decir una intimidad que nace del individualismo exigiendo respeto de los demás a ser aquella libertad positiva en donde el ciudadano tiene la facultad o el derecho de controlar su información personal **(Piñar Mañas, 2006)**.

4.4.5. Buenas prácticas en México

En el caso de la normatividad mexicana, esta expresa en la constitución de forma clara y contundente el derecho a salvaguardar la información personal en el artículo 14 que se refiere al tema de la siguiente manera:

"Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros **(Constitución Política de los Estados Unidos Mexicanos, 1917)***"*

Dicha disposición deja claro el derecho a la protección de los datos personales y establece el punto de partida para verificar el cabal cumplimiento de dicho orden constitucional.

Los rasgos más acentuados de la normatividad que sigue, Nueva Ley DOF 26-01- 2017,Ley General de Protección de Datos Personales en posesión de sujetos obligados **(Presidencia de la República, 2017)**, tienen que ver con el modo expreso o tácito con el que se puede recabar el consentimiento y las características de su validez, en este sentido se asemeja a los derechos **ARCO** contemplados en la Constitución en el artículo 16 que son los derechos de Acceso, Rectificación, Cancelación y Oposición a la información que manejan los particulares **(CEPAL, 2010)** en cuanto se destaca su régimen necesario y estricto con respecto a los deberes de obligatorio cumplimiento para el administrador de los datos personales.

Se destaca además la dedicación normativa con ocasión de la brecha de seguridad necesaria para la protección de la información, así como en lo que tiene que ver con vulneraciones y régimen sancionatorio.

Tabla 2 Cuadro resumen de principales aportes de buenas prácticas en EEUU y Latinoamérica

País	Leyes sobre protección de datos	Principales aportes
EEUU	-Constitución de Estados unidos, primera enmienda. - Common Law Rigtht to Privacy	-Está centrado en la protección de la privacidad. -Da la libertad al ciudadano de Abstenerse en caso de información de origen ideológico. -El ciudadano escoge que parte de su información

		personal quiere que sea expuesta. -Limita el uso abusivo de tecnologías.
Argentina	-Ley 25.326 del 2 de noviembre del 2000. .-Ley 1.845 de Protección de Datos Personales, Ciudad Autónoma de Buenos Aires.	-Nombra expresamente en la constitución el derecho del ciudadano a conocer la finalidad de sus datos personales. -Tiene gran influencia de la Legislación europea al respecto.
Uruguay	-Ley No. 18.331, de 11 de noviembre de 2008. Decreto 414/009	-El titular de la información puede ser una persona jurídica. -Propone como principal punto de partida la intimidad del individuo. -Tiene gran influencia europea.
Perú	Ley No. 29733, de 3 de julio de 2011, de Protección de Datos Personales.	-Nombra expresamente en la constitución, el derecho del ciudadano a solicitar y recibir información. -El régimen sancionatorio tiene infracciones y Sanciones. -Los derechos del ciudadano frente a la protección de sus datos personales son más amplios. -Previsión de la injerencia de la informática.
Venezuela	Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal y el Real Decreto 1720/2007,	-explora la posibilidad de que la informática sea una amenaza a la intimidad y pone límites a su aplicación. -El ciudadano tiene la facultad de controlar su información personal.
México	Nueva Ley DOF 26-01- 2017 – Ley General de Protección de Datos Personales en posesión de sujetos obligados	-Se enuncia en la constitución de forma clara como derecho fundamental.

	-es estricta con los deberes y la obligatoriedad del cumplimiento de los administradores frente al tratamiento de datos personales. -se destaca la seguridad frente a la protección de la información, con un régimen sancionatorio estricto.

Tabla No 2: Elaboración Propia en base a referencia bibliográfica.

4.4.6. Generalidades y análisis de buenas prácticas Latinoamericanas

Como se ha evidenciado, en la base normativa latinoamericana se reconoce bien sea de forma tácita o expresa el derecho que todo ciudadano tiene sobre los datos personales suministrados a bancos de datos privados o públicos, con las restricciones que establece la ley para este último caso.

De igual modo, se estudia y analiza la confidencialidad que debe tener la información, así como el conocimiento del titular de los datos, respecto del uso, rectificación, actualización o supresión de la información suministrada.

No obstante, dichas características no son acogidas en su conjunto por todos los países latinoamericanos, unos como Argentina y Uruguay guardan relación estrecha con el respeto a la intimidad, pero no incluyen la informática como factor de riesgo, mientras en países como Perú y Venezuela se tiene en cuenta el contexto tecnológico, pero se desconocen factores claves en cuanto a la implementación de la ley y su apartado sancionatorio.

Así, la mayoría han adoptado normas de protección de datos personales de forma aislada **(CEPAL, 2010)**, como parte de la normativa sectorial, pero no la han incluido en su marco

constitucional, ni como derecho fundamental, de modo tal que la normatividad latinoamericana, sigue presentando falencias en lo que respecta a la gestión de la seguridad de datos personales.

5. Prospectiva de normatividad y gestión de la seguridad de la información de Datos personales

5.1. Diagnóstico y evaluación de la normatividad actual en torno a la protección de datos personales.

Después de revisar con detenimiento la parte documental y legislativa de la gestión de la seguridad de datos personales en Colombia y de analizar las buenas prácticas internacionales, es necesario generar un diagnóstico, por medio de una consulta a una muestra representativa, acerca de su conocimiento y percepción sobre el tratamiento y administración de su información, con el fin de obtener mayor fundamentación al generar el análisis final y las recomendaciones para una nueva normativa en el tratamiento y gestión de los datos personales, a partir de todo lo anterior.

La herramienta metodológica utilizada para este propósito fue un formato de encuesta, con nueve (9) preguntas cerradas, aplicadas a un grupo de ciudadanos bogotanos, mayores de 18 años elegido de forma discrecional, la aplicación se realizó a ciento seis (106) personas entre hombres y mujeres profesionales en diferentes áreas del saber.

5.2. Metodología:

El presente trabajo investigativo se realizó empleando una metodología de tipo mixta, en la que se pretendió comprender y analizar la doctrina y los diversos factores que influyen en la producción normativa y jurisprudencial, a partir de un análisis en torno a la investigación de la situación de la gestión de la seguridad de datos personales, por otro lado, se tenía como fin indagar cuantitativamente sobre el público que regularmente debe someter sus datos personales

en sitios comerciales y transacciones cotidianas, a fin de generar un diagnóstico sobre la percepción y el efecto social producido en el contexto actual.

El trabajo desarrollado se sustenta desde las bases teóricas de la importancia de la protección de los datos personales, el derecho a la intimidad personal, el buen nombre y la privacidad individual y familiar, estos aportes nos permiten validar la postura de la investigación y así avanzar en el objetivo del estudio.

En cuanto al diseño metodológico, se planteó como descriptivo y exploratorio, pues se basó en la observación del fenómeno estudiado y en el análisis y registro detallado de los acontecimientos; además de esto, se exploraron de forma general los diferentes factores normativos que intervienen en la legislación colombiana y se indago además sobre las buenas prácticas que se han evidenciado a nivel internacional, con el fin de aproximarse a la intención u objetivos de las mismas.

Por otro lado, para establecer reflexiones y conclusiones en torno a la importancia, retos y perspectivas de la gestión y protección de datos personales, fue necesario un análisis desde el contenido que lo sustenta, y para este fin se utilizó la investigación cualitativa, pues es un proceso interpretativo de indagación que hace énfasis en la descripción, clasificación y explicación, **(Cerda Gutiérrez, 2000)**, lo cual facilita el análisis de lo consignado en la investigación a través de los referentes teóricos, permitiendo establecer los criterios de revisión y contrastarlos con la bibliografía, para después facilitar la generación de la hipótesis.

5.2.1 Fases de Diagnóstico

Lo anterior se ejecutó en una FASE 1, a partir de la revisión documental de gran variedad de documentación doctrinal, jurisprudencia y normatividad a nivel nacional e internacional

referentes al tema de la protección de datos personales, este procedimiento denominado bibliometría y se basa en la necesidad de efectuar un recuento de la documentación existente, buscando rasgos característicos y líneas comunes entre ellos, **(Carrizo Sainero, 2000)**.

En la FASE 2, se analizó la normatividad existente, a la luz del marco teórico de la presente investigación, con miras a determinar los factores de coincidencia y disonancia entre ellos, es decir el análisis cualitativo de la información a partir de los principales referentes académicos señalados en la presente investigación.

En la FASE 3 se indagó sobre la percepción y generalidades de la protección de datos personales, por medio de un cuestionario aplicado de manera aleatoria a diferentes usuarios del común, por medio de la aplicación de mensajería para teléfonos inteligentes Whatsapp y correo electrónico, con el fin de establecer el conocimiento e interpretación de los usuarios que generalmente deben aportar sus datos en transacciones cotidianas.

5.2.2. Herramienta metodológica

En cuanto a la herramienta metodológica usada para la recolección de información, se planteó un cuestionario semiestructurado, en el que se presentan nueve (9) preguntas con dos opciones de respuesta, con el fin de obtener la información necesaria para cumplir con los objetivos de la investigación.

Este cuestionario (Anexo 1) permite además, ir más allá de la observación y obtener resultados que se pueden cuantificar, por eso y gracias a este instrumento, se logró consolidar y verificar la información consignada en la parte final de la investigación, la población entrevistada fue escogida por un método no probabilístico, entre los usuarios frecuentes de transacciones

comerciales en donde tienen que brindar sus datos personales, se tomó como muestra la aplicación de la herramienta a ciento seis (106) personas.

5.2.3. Población objetivo

En el diseño muestral se tuvieron en cuenta ciento seis (106) personas escogidas de forma aleatoria, quienes resolvieron el cuestionario por medio de la aplicación de mensajería para teléfonos inteligentes Whatsapp y correo electrónico .

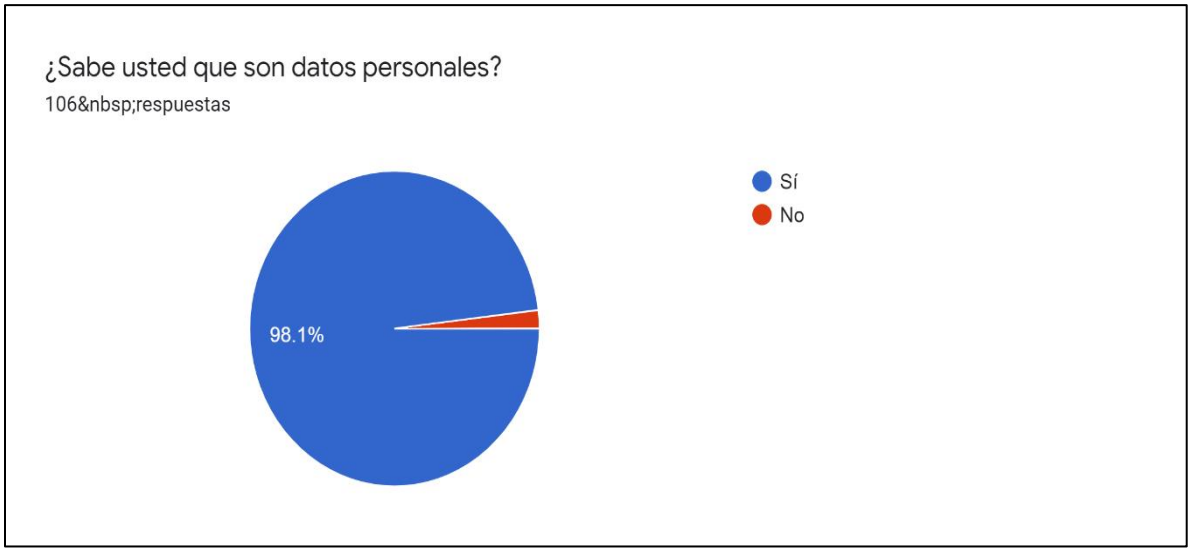
5.2.4. Diseño Muestral

El estudio se realizó en la ciudad de Bogotá, la intención principal fue generar un diagnóstico sobre la población que cotidianamente debe brindar sus datos personales en transacciones comunes y de esta manera avanzar hacía los objetivos trazados para la presente investigación.

La estructura tenía la intención de informar con un breve encabezado los derechos del usuario frente a la protección de datos personales: rectificar, actualizar y conocer, al mismo tiempo que indagaba sobre los saberes y percepciones de los ciudadanos sobre el tratamiento y gestión de datos personales, la difusión se realizó por medio de la aplicación de mensajería para teléfonos inteligentes Whatsapp y correo electrónico.

A continuación, se muestran las preguntas y los resultados obtenidos en el diagnóstico:

Gráfico 1: Pregunta 1 de Consulta Sobre Datos Personales



Grafica No 1: Elaboración propia en base a resultados.

En la primera pregunta relacionada con el conocimiento del usuario frente a los datos personales en general, se evidenció que en su mayoría (98,1 %), de las personas tienen conocimiento sobre el concepto de datos personales, mientras una muy mínima proporción (1.8%) no tienen conocimiento sobre su significado.

Se evidencia entonces, el conocimiento general sobre datos personales, entendido como toda información de carácter personal, que compete al individuo.

Gráfico 2: Pregunta 2 de Consulta Sobre Datos Personales

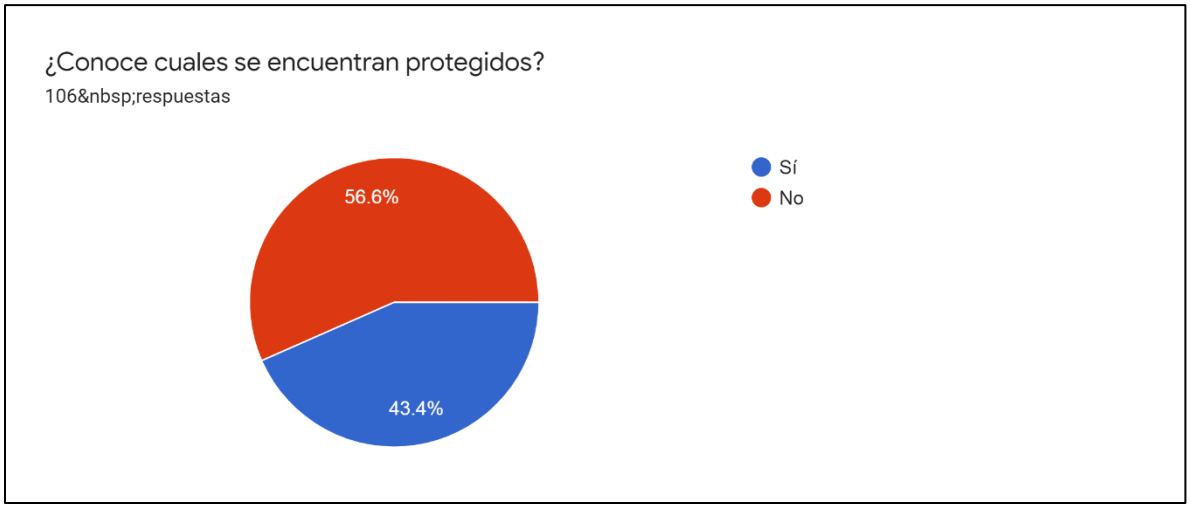


Gráfico 2: Elaboración propia basada en resultados de diagnóstico.

En la segunda formulación concerniente cuales de los datos personales se encuentran protegidos, los resultados mostraron una proporción casi igual entre los usuarios que tienen conocimiento sobre la información que tiene protección (43.4 %), y los que no sabían de dicha clasificación (56.6 %), siendo levemente mayor el desconocimiento sobre este punto.

Se evidencia de manera general, en esta y en otras preguntas el desconocimiento general sobre la ley de protección de datos personales, si bien el desconocimiento de la ley no es excusa, si es obligación de la superintendencia socializar el contenido de la misma.

Gráfico 3: Pregunta 3 de Consulta Sobre Datos Personales

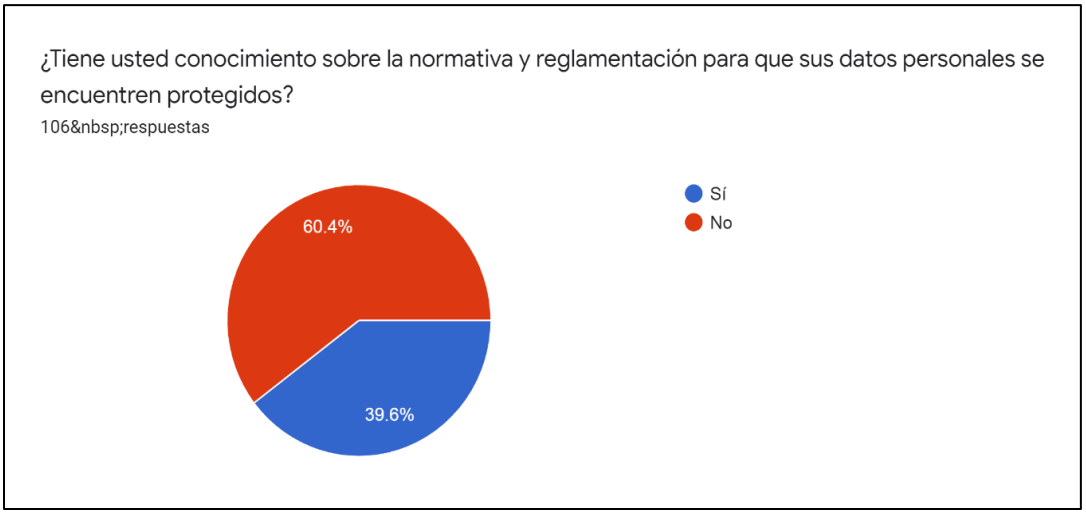


Gráfico 3: Elaboración propia basada en resultados de diagnóstico.

Al indagar sobre el conocimiento sobre la normativa y reglamentación de la norma, una proporción alta de usuarios (60.4%) afirmaron no poseer información al respecto, mientras el porcentaje restante (39.6%) sostuvieron que si la conocen.

Hay que resaltar en este punto, que si bien, la superintendencia ha procurado realizar cartillas informativas, sobre los principales aspectos, la mayoría de la población sigue sin conocer el contenido de la ley.

Existe desconocimiento frente a la legislación en la protección de datos personales por parte de sus titulares en tal sentido se evidencia una escasa divulgación frente a la misma, lo que conlleva que se presente mayor vulnerabilidad en su seguridad.

Gráfico 4: Pregunta 4 de Consulta Sobre Datos Personales

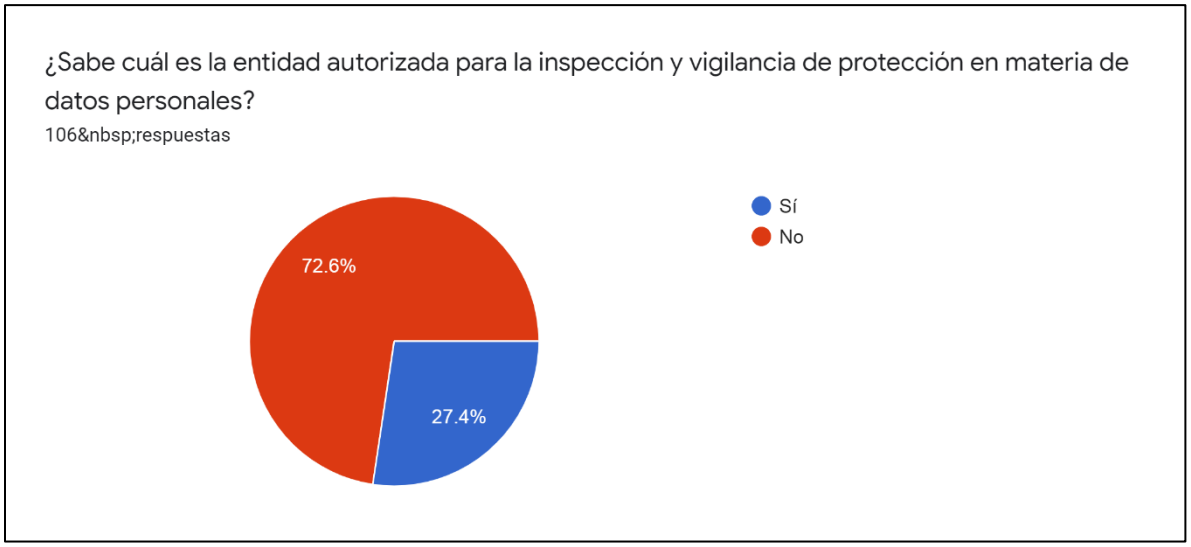


Gráfico 4: Elaboración propia basada en resultados de diagnóstico.

Con respecto a la pregunta sobre la entidad encargada del cumplimiento de la noma, solamente un (27.4%) tiene conocimiento de que es la Superintendencia de Industria y Comercio, el resto de los usuarios consultados, es decir la mayoría (72.6) desconocen el ente de control al cual pueden acudir en caso de presentarse vulneración a la protección de sus datos personales.

Un indicador bastante diciente, frente a la cantidad de casos que pudieran presentarse, donde el titular del dato desconociera el ente de control correspondiente.

Gráfico 5: Pregunta 5 de Consulta Sobre Datos Personales

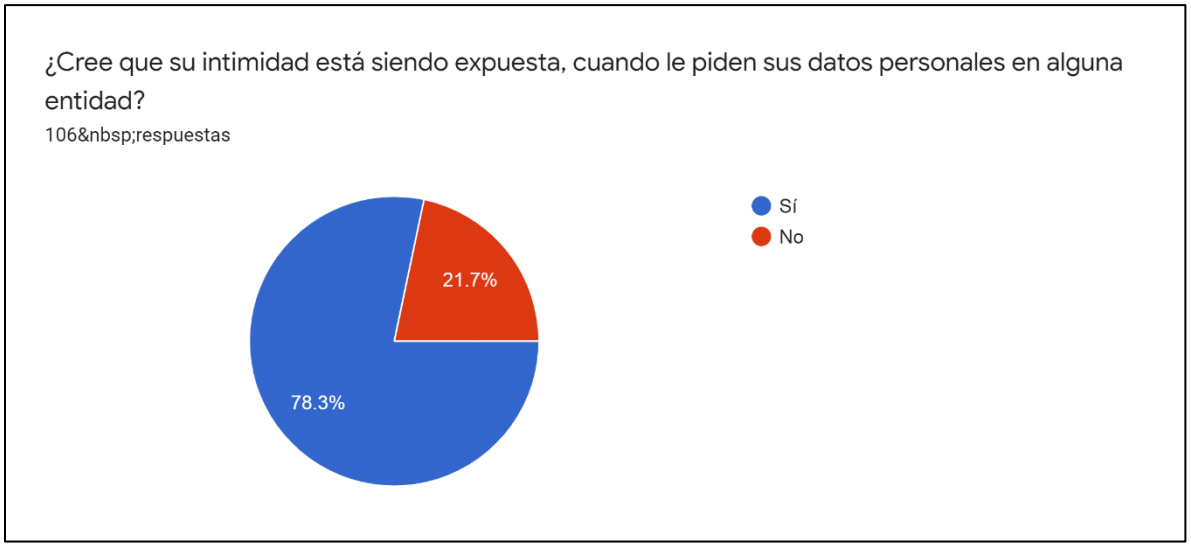


Gráfico 5: Elaboración propia basada en resultados de diagnóstico.

Al indagar sobre la percepción del usuario con respecto a la exposición de su intimidad, al brindar sus datos en diferentes entidades, solo el (21.7%) no ven comprometida su intimidad, mientras la gran mayoría (78.3%) consideran que está siendo expuesta siempre, cuando le solicitan la información personal.

Respecto a ello, la norma dicta su disposición en el sentido de que los datos personales deben tener un fin específico, sin embargo, el parecer colectivo indica que en la mayoría de los casos su información personal, termina en manos de terceras personas.

Gráfico 6: Pregunta 6 de Consulta Sobre Datos Personales

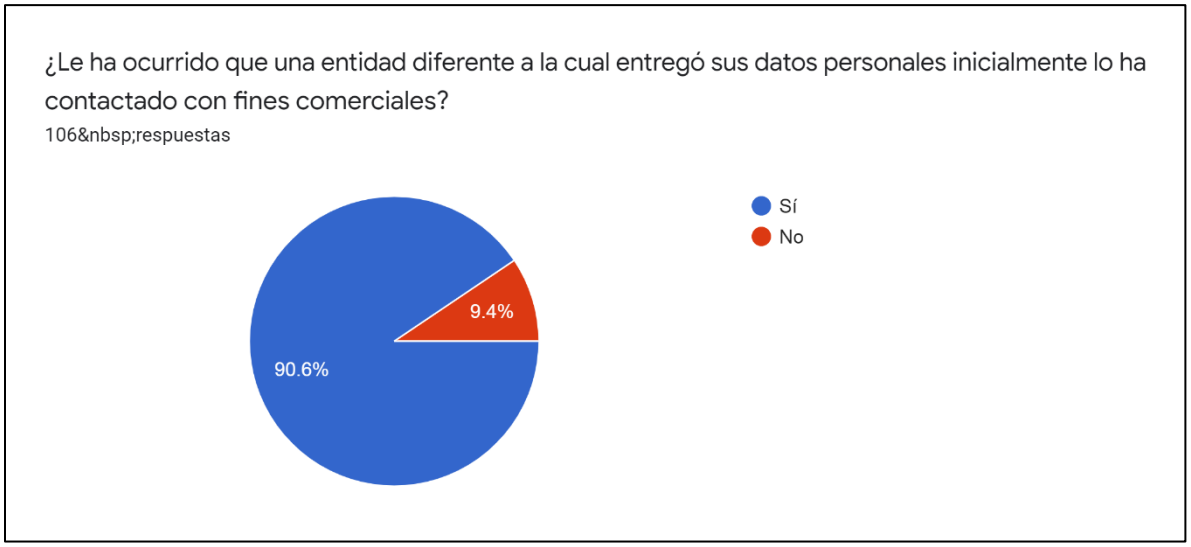


Gráfico 6: Elaboración propia basada en resultados de diagnóstico.

Frente a la pregunta sobre la posibilidad de que otra entidad diferente a la que en un inicio recolecto los datos del titular, lo contacte, la gran mayoría (90.6%) afirmo haber pasado por la situación, mientras tan solo un (9.4%) no contempla la posibilidad.

La falta de claridad en la norma y la reglamentación que la lleva a cabo, no ha establecido los limites suficientes para evitar que esto suceda, de tal manera que muchos de los administradores de datos, presentan falencias frente al cabal cumplimiento del principio de finalidad, que debe salvaguardar los derechos de los titulares del dato.

Gráfico 7: Pregunta 7 de Consulta Sobre Datos Personales

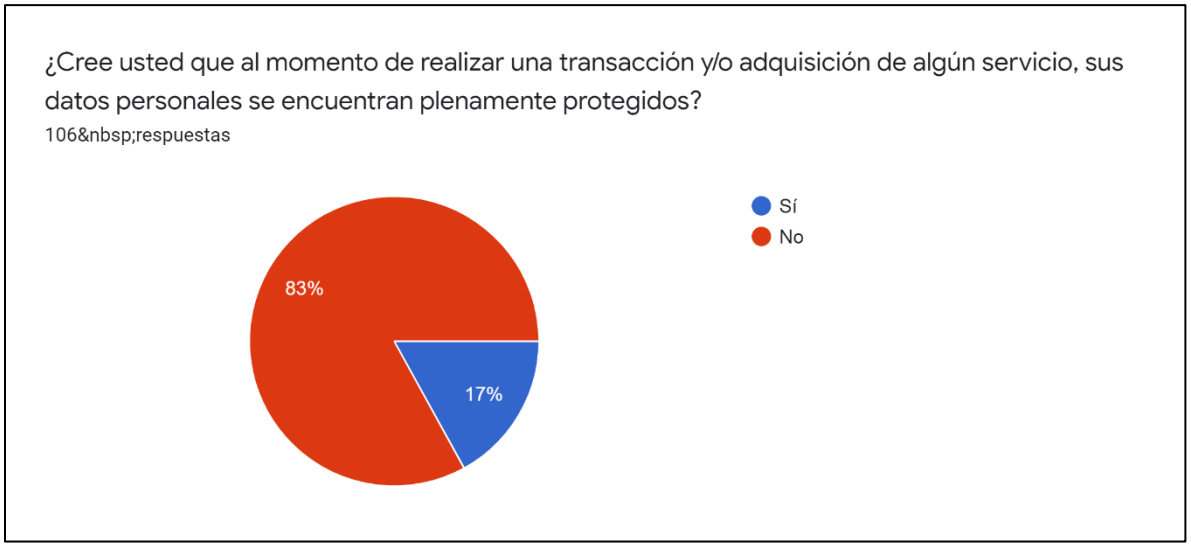


Gráfico 7: Elaboración propia basada en resultados de diagnóstico.

En cuanto a la percepción del ciudadano frente a la protección de los datos personales al momento de realizar una transacción o adquirir algún producto o servicio, solo una quinta parte (17%) cree que su información personal está protegida, mientras el restante (83%), una proporción mucho más grande, cree que sus datos no se encuentran plenamente protegidos.

Lo anterior evidencia que en múltiples ocasiones la información del titular del dato es usada de forma indiscriminada, generando desconfianza, frente a la protección de datos, al momento de realizar cualquier transacción y/o adquirir algún servicio.

Gráfico 8: Pregunta 8 de Consulta Sobre Datos Personales

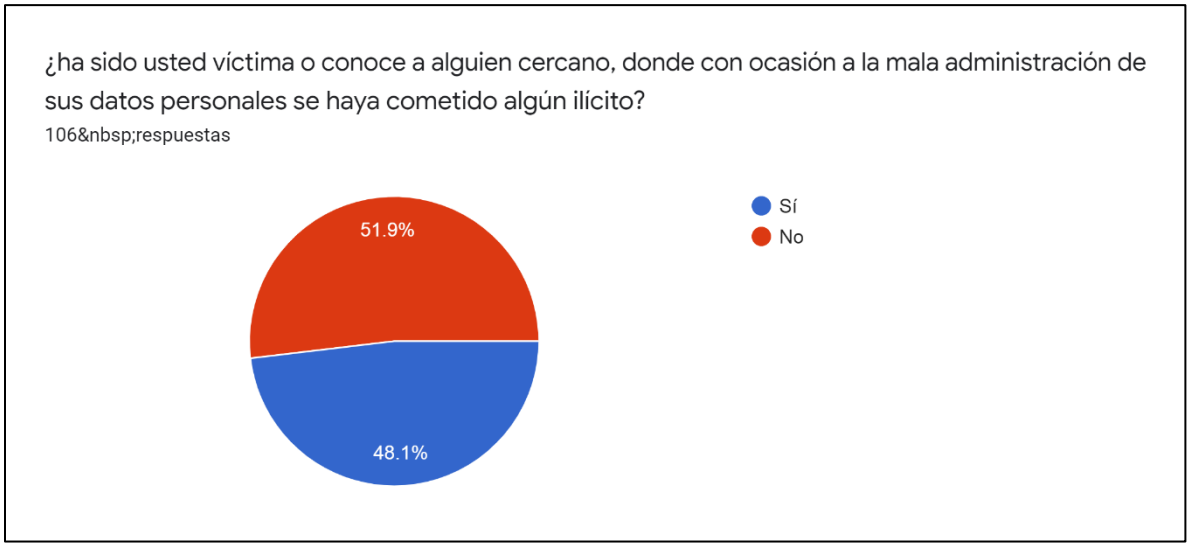


Gráfico 8: Elaboración propia basada en resultados de diagnóstico.

En cuanto a la cercanía de la comisión de un ilícito, en persona propia o alguien cercano, el diagnóstico indicó, que aproximadamente la mitad de los usuarios consultados (51.9%) tiene conocimiento de algún caso en referencia, mientras un (48.1%) no conoce sobre ilícitos en torno a la indebida administración de la información personal.

Lo anterior evidencia la poca seguridad que existe, en cuanto a la finalidad de los datos personales, la indebida administración de estos y la recurrencia de poca protección en el proceso de recolección de información personal.

Gráfico 9: Pregunta 9 de Consulta Sobre Datos Personales

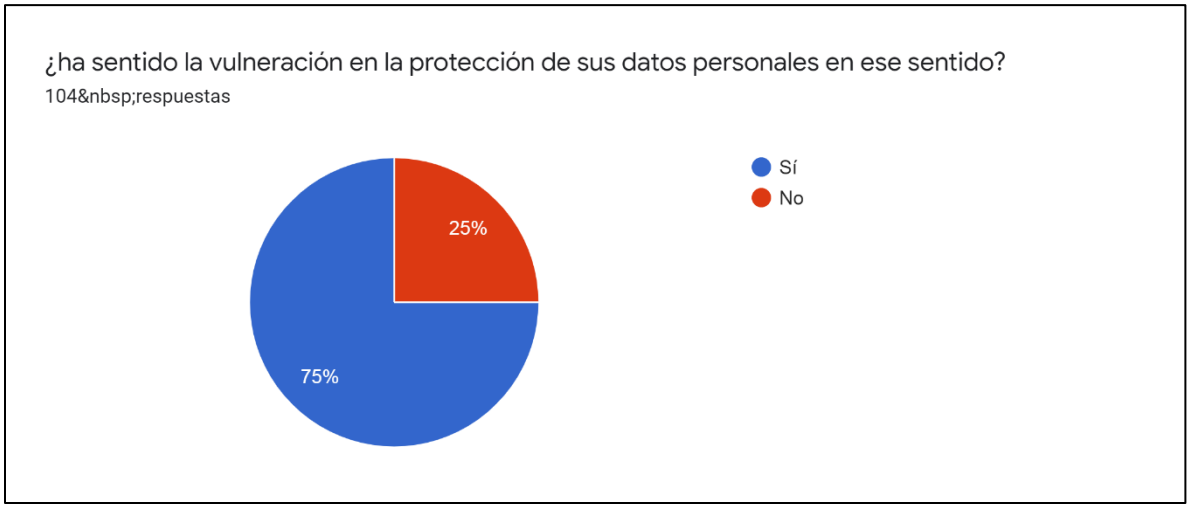


Gráfico 9: Elaboración propia basada en resultados de diagnóstico.

Referente a la percepción que tienen los ciudadanos con respecto de la vulneración de sus derechos en cuanto al ámbito penal o la comisión de ilícitos, con ocasión a la carencia en la protección en el tratamiento de datos personales, una inmensa mayoría (75%) siente que ha sido vulnerado, mientras tan solo el (25%) tiene una percepción de seguridad en referencia a ello.

Se evidencia también a lo largo de este diagnóstico, que a partir de la falta de protección hacia los derechos que se desprenden de la administración de datos personales, como son la intimidad o el buen nombre, se derivan la comisión de ilícitos y que gran parte de la población que debe entregar su información, en las transacciones diarias, para acceder a bienes y servicios se ve expuesta a este tipo de fenómenos, a causa de la falta de claridad en la delimitación de la protección a los datos personales y la poca trascendencia en cuanto a su régimen sancionatorio.

5.3.Análisis y Necesidades Normativas detectadas.

Nuestro país ha progresado paulatinamente en los últimos años en cuanto a la gestión de la seguridad de los datos personales, gracias a la normativa y procesos jurisprudenciales que se dedican a proteger los derechos fundamentales, así como a la implementación de recursos y procedimientos para su salvaguarda.

Fue a partir de la jurisprudencia que empezó a destacarse el derecho de habeas data como un derecho autónomo que se distingue de otros derechos igualmente fundamentales como el buen nombre o la intimidad **(Corte Constitucional, 2011)**, sin embargo a nivel internacional se vienen dando evoluciones, en cuanto a las estrategias que garanticen la seguridad jurídica sobre el tema, por ello esta construcción alrededor de la protección de la información personal ha sido el foco de discusiones legislativas que claramente evidencian la ausencia de contenidos normativos apropiados y eficaces para la tutela de este derecho.

5.3.1. Tecnología y protección de datos:

Una de las principales necesidades normativas detectadas, tiene que ver, con la cada vez más invasiva naturaleza de la informática en el mundo moderno **(Alvarez, 2015)**, lo que deriva en el paulatino surgimiento de nuevos riesgos para los individuos en cuanto a la protección de su intimidad y de su información personal, existe entonces, una clara necesidad en el sentido de perfeccionar las disposiciones existentes, en busca de corresponder adecuadamente a las necesidades contextuales de globalización.

En la actualidad, se generan cada día nuevas y más diversas formas de procesamiento y recolección de datos, gracias a la red, es sencillo acceder a la información personal y comercial de los individuos, lo que ha permitido el acceso de otro tipo de actividades como las delincuenciales **(Alvarez, 2015)**, a falta de la regulación adecuada, por ello es determinante proteger la intimidad frente a las nuevas tecnologías y garantizar la protección de sus derechos al usar los medios informáticos.

En el capítulo de buenas prácticas internacionales, se observa como los países europeos han mostrado una preocupación coherente con el aumento de las nuevas tecnologías y han buscado proteger los derechos de los usuarios frente a estas herramientas, ejemplo de esto es España donde el alto tribunal hizo énfasis en lo siguiente:

"Debe defenderse fundamentalmente el honor y la intimidad, pero también de una herramienta que es, en sí misma, un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la libertad de la persona proveniente de un uso ilegítimo del tratamiento mecanizado de datos, lo que la Constitución llama la informática **(Parlamento Europeo, 1995)**"

Así, tanto la legislación española, como la alemana y portuguesa señalan límites a la actividad informática que se contraponga a los derechos de los ciudadanos, mientras que, en Latinoamérica, unos pocos países, solo Perú y Venezuela han previsto la injerencia de la informática en la intimidad de las personas y lo han hecho de forma tácita, en Colombia se hace necesario que la normativa se adapte al contexto, procurando alternativas legales que impidan que los derechos de los titulares del dato se vean comprometidos.

5.3.2. Falencias en los principios:

Los principios, como se ha dicho deben ser la base para la protección de los derechos en materia de datos personales, por tanto, su deber ser debería estar encaminado hacia la cobertura de todas las necesidades que se presenten al respecto **(Corte Constitucional, 2011)**, teniendo en cuenta que ellos enmarcan la actuación general sobre la información personal de los ciudadanos, no obstante, el presente trabajo investigativo ha detectado diversas fallas en cuanto a:

Principio de finalidad: este es el principal aspecto a regular, toda vez que este presentan falencias, pues no se está haciendo uso del dato con el propósito para el cual fue recolectado y terminando a merced de terceros, siendo objeto de uso con fines diferentes al indicado por el titular del dato inicialmente.

Principio de libertad: el cual va de la mano al anterior, toda vez que el consentimiento que se otorga al momento de la recolección del dato, se encuentra desviado por no establecerse claramente a que terceros se autoriza para suministrar o divulgar la información.

Principio de circulación restringida: se evidencia vulneración de este principio, cuando los datos del ciudadano quedan a disposición de terceros, sin autorización previa y concreta por parte del titular.

Principio de seguridad: Todo lo anterior conllevando al incumplimiento del principio de seguridad, pues, no se evidencia que el dato suministrado por el titular se encuentre protegido, siendo este vulnerable al uso indiscriminado y expuesto a posibles fines indebidos.

5.3.3. Falta de claridad en los límites:

Algunas de las falencias más destacadas, se presentan por la falta de claridad en los límites, por cuanto la **Ley 1581 de 2012** señala en el objeto en el artículo 1, en aras de proteger el derecho constitucional a la intimad articulo 15 y a la información artículo 20, que se debe incluir dentro de los derechos, de conocer, actualizar y rectificar el derecho a autorizar el uso concreto de los datos **(Congreso de la República, 2012)**, toda vez que precisamente al no existir claridad en la aplicación y delimitación del mismo, se encuentra un vacío, generando la alta probabilidad de que se desvíe la finalidad para la cual fue recolectado el dato.

Así mismo se evidencia que el articulo 8 en su literal b. de la ley se encuentra sin base alguna teniendo en cuenta que el soporte que señala como prueba de autorización se encontraría en contra del titular del dato, por cuanto dicha autorización no fue especifica o concreta frente al servicio o transacción efectuado, toda vez que al momento de dicha autorización no se garantizó la protección del dato y el uso exclusivo del mismo o su finalidad concreta.

Para este caso es importante señalar la buena práctica de empresas colombianas como Cine Colombia S.A. quienes, al momento de suscripción en la página de internet, dan cabal cumplimiento al deber ser de la autorización concediendo la opción al suscriptor o titular del dato de recibir información adicional de otros servicios lo que determina que el dato se va a suministrar solo a lo que autorice especialmente el titular del mismo.

Sin embargo, esto se determina discrecionalmente depende de la empresa, que preste el servicio, en este caso, mientras Cine Colombia S.A. hace lo propio, Cinépolis que se encuentra a cargo de Operadora Colombiana de Cines S.A, otra empresa que presta el mismo servicio, solo

hace mención a sus términos y condiciones de uso y en ningún aparte de su página señala la Ley 1581 de 2012 referente a la protección de datos personales, se limita solamente a solicitar la autorización, así se autoriza el uso de datos personales asumiendo que solo serán utilizados para boletos y comida en las salas de cine de esta empresa sin mayores garantías.

En el caso de Cinemark Colombia S.A. se habla de servicios indirectos sin especificar cuáles como debería hacerlo, de tal manera que no se conoce la finalidad del uso del dato.

Así las cosas, se encuentra que el cumplimiento de la norma como tal por parte de ciertas entidades no es suficiente para garantizar la protección de los datos personales cuando si bien es cierto el ente de control se encuentra señalando unos parámetros **(CEPAL, 2010)**, también lo es que no ha sido suficiente por cuanto no se evidencia que establezca una obligatoriedad concreta al momento de la autorización.

5.3.4. Falta de rigurosidad en la aplicación de sanciones:

Al no existir claridad en la normativa general sobre protección de datos, se presentan inconvenientes en cuanto a la aplicación de sanciones **(Piñar Mañas, 2006)**, dado que no están bien definidos los limites sobre los cuales debería actuar el organismo de control, por lo tanto, Falta rigurosidad en su aplicación.

Ahora bien, la labor de la Superintendencia de Industria y Comercio, se ve perjudicada, al no contar con una base normativa sólida, que le permita ejercer sus funciones a cabalidad, máxime cuando no se ha socializado adecuadamente las funciones y competencia de la misma, es necesario informar adecuadamente a las entidades que recolectan y administran los datos personales y fomentar el uso de información concreta dentro de los formatos de autorización implementando y generando garantías frente a la seguridad de la información que se está

suministrando, de tal manera que el titular el dato no tenga que acudir a reclamaciones engorrosas, atribuyéndole los vacíos de la normatividad asumiendo dichas falencias.

6. Conclusiones y Recomendaciones para la optimización de la normativa en protección de datos personales.

Cada ser humano es un mundo diverso, en el que se entretejen muchas circunstancias inherentes al desarrollo de su personalidad, es normal entonces, que a lo largo de toda su vida genere información variada sobre sus saberes gustos, propósitos e información de todo tipo, en la actualidad gracias a los medios tecnológicos y a la llamada democratización de la información, es cada vez más fácil acceder a dicha información, a partir de lo anterior resulta en muchas ocasiones fácil, encasillar o tratar de interpretar el individuo a través de sus datos personales, lo que llevaría fácilmente a problemáticas más peligrosas, al existir la posibilidad de generarse problemas sociales como la exclusión o la manipulación frente a sus tendencias ideológicas o de naturaleza sexual, entre otras.

Por ello la rigurosidad en la norma de protección de datos debe ser tan exhaustiva **(Remolina Angarita, 2013)**, pues su importancia es notoria en cuanto a la protección de derechos fundamentales como la intimidad y el buen nombre, para ello después de un trabajo riguroso se ha llegado a las siguientes conclusiones, en aras de la optimización de la base normativa, en la gestión de la seguridad de datos personales.

6.1.Previsión del Uso de la informática

Algo que es esencial en, es el estudio de las buenas prácticas internacionales, que han dado paso a grandes progresos en torno a la normatividad en general y también en lo que se refiere específicamente a la protección de datos personales, uno de esos factores es la prevención de la injerencia de las nuevas tecnologías en la intimidad de las personas.

Como se ha anotado, los países europeos han estudiado y llegado a normativas concluyentes frente al fenómeno de la informática **(Rivera Llano, 2008)** y han generado limites adecuados respecto a la prevención de que los grandes avances interfieran en la cotidianidad intima de las personas.

Según los preceptos europeos el derecho del ciudadano a preservar el control sobre sus datos personales y la limitación de la informática frente a la intimidad, debe ser el marco en el cual el legislador consagre de manera efectiva, el derecho fundamental a la protección de datos de carácter personal.

De tal modo, es imperioso incluir el análisis del factor tecnológico de forma amplia y concluyente en la legislación colombiana sobre protección de la información personal, a fin de establecer límites y proteger el derecho fundamental de la intimidad y más allá de este, el derecho sagrado de la dignidad del ser humano.

6.2.El derecho de protección de datos personales como fundamental.

En la misma lógica europea, la protección de datos se enmarca como fundamental y se expresa de forma clara y contundente en su legislación **(Alvarez, 2015)**, en nuestro país debería aplicarse

este ejemplo adaptándolo al contexto, ya que la formulación de derecho fundamental, garantizaría la protección jurídica de los derechos de las personas con respecto a su información personal, que entre otros podría generar reclamación más efectiva frente al acceso, rectificación, oposición y cancelación de sus información personal, ante la inminente inmiscusión de las nuevas tecnologías.

6.3.La inclusión de la autorización:

Como se ha mencionado con anterioridad, es necesario crear las herramientas normativas que señalen la obligatoriedad de la autorización, con el fin de garantizar la trazabilidad y conveniencia jurídica, en la protección de los derechos de los titulares del dato.

Por tanto, es necesario, especificar como se debe llevar a cabo la autorización, ya que como se encuentra consignada actualmente en el artículo 9 de la ley **(Congreso de La República, 2013)**, no tiene el soporte legal adecuado, de esta forma se garantizaría la protección del dato recolectado, lo mismo tendría que aplicarse al artículo 12 cuando se refiere al deber de informar al titular, pues en la mayoría de los casos al realizar una transacción, no se especifica la finalidad del uso del dato.

En ese mismo sentido, se evidencia que es escaso lo señalado en el artículo 17 de la ley en su literal c. cuando indica que el responsable del dato garantiza al titular la finalidad de la recolección del mismo, que a su vez debe ser informada y sus derechos frente a dicha autorización, así como la señalada en el literal d. al momento de garantizar la seguridad del dato en cuanto a su uso, consulta o acceso por parte de terceros con el fin de impedir la adulteración entre otros del mismo.

Por tanto, el **Decreto 1377 de 2013** debería brindar cumplimiento a lo señalado en el artículo 5 que refiere a la autorización en cuanto a la finalidad específica para el tratamiento de datos y que en caso de efectuarse cambios en las políticas de tratamiento el responsable del tratamiento debe informar al titular y obtener una nueva autorización cuando dicho cambio se refiera a la finalidad del tratamiento.

Así mismo el artículo 7 del decreto señala que el modo de obtener la autorización debe ser por escrito o de forma oral **(Congreso de La República, 2013)** y mediante conductas inequívocas este último muy amplio en su concepto por cuanto como se evidencia no se cumple a cabalidad por cuanto la finalidad del tratamiento de los datos recolectados se presumiría por parte del titular que solo van a ser utilizados para el servicio o transacción adquirido sin ninguna garantía específica respecto de otros usos.

6.4.Autodeterminación:

Muy importante dentro de la normatividad tanto europea como de Estados Unidos es la capacidad del usuario de decidir cuales datos entregar **(De la Calle Restrepo, 2008)**, en España la ley impone a los terceros administradores intervinientes imposiciones expresas sobre los deberes jurídicos, para la protección de los derechos de los ciudadanos.

Así mismo, está la obligatoriedad de dar a conocer la facultad de autodeterminación referente a su información personal, lo cual permite a los ciudadanos garantizar el control autónomo sobre sus datos personales, lo que solo es factible al generar la imposición de obligatoriedad de realizar esa mención expresa.

En caso tal, tendrían que ser mencionados: el derecho a que se requiera el previo consentimiento para la recolección y uso de los datos personales, el derecho a saber y ser informado sobre el destino y uso de esos datos y el derecho de acceder, rectificar y cancelar dichos datos. En definitiva, el poder de disposición sobre los datos personales.

6.5.La privacidad como derecho fundamental

De acuerdo con lo analizado a través de este trabajo de investigación, en países como Estados Unidos concede una prevalencia especial a la privacidad de las personas **(Nieves Saldaña, 2011)**, esta característica se protege principalmente en países cuyo desarrollo socio económico es muy alto, así también desde la ONU se ha venido haciendo énfasis en la necesidad de implantarlo en la legislación de los países como derecho fundamental, consiguiendo un impacto cada vez mayor, en este sentido en la unión europea, que ha adoptado esta proposición, ajustándolo a la normatividad general de los países europeos.

En este contexto, además de haber adaptado la legislación al contexto globalizado, encontramos grandes avances en cuanto a la protección de la privacidad de los ciudadanos, de hecho, nos encontramos ante el instrumento normativo que más se preocupa por la protección de este derecho **(Remolina Angarita, 2013)**, por una parte, por la capacidad de cubrimiento o ciudadanos a los que ampara y por otro por la homogeneidad de protección que presenta.

Así pues, es necesario recalcar la inclusión de la privacidad y la protección de datos personales como derecho fundamental, como prueba ineludible de la democratización global en la materia.

Colombia no puede ser ajeno a este propósito y debe involucrar estos valores de gran importancia para el ser humano, a fin de cubrir efectivamente los derechos respecto a la

protección de datos personales, generando una normatividad que mejore en los aspectos mencionados y que tenga como eje central, la protección de la intimidad y la privacidad de los ciudadanos.

7. Bibliografía

Alvarez, G. (2015). *Seguridad Informática para empresas y particulares.* Madrid: Mc Graw Hill.

Boletin Oficial Federal. (1949). *Grundgesetz.* Bonn.

C - 1011 (Corte Constitucional 2008).

Cáceres, P. (2003) *Análisis cuantitativo de contenido: una alternativa medológica alcanzable.* Chile. Pontificia Universidad Católica de Valparaíso.

Carrizo Sainero, G. (2000) *Hacia un concepto de Bibliometría*. Madrid: Universidad Carlos III.

Cerda Gutiérrez, H. (2000). *Los elementos de la investigación, como reconocerlos, diseñarlos y construirlos.* Bogotá: Editorial El Buho.

Camargo, P. (2015). *El habeas Data: derecho a la intimidad.* Bogotá: Leyer.

CEPAL. (2010). *Panorama del Derecho Informático en America Latina y el Caribe.* Santiago de Chile: Naciones Unidas.

Congreso de la República. (1991). Constitución Nacional de Colombia. Bogotá: Legis.

Congreso de la República. (18 de Octubre de 2008). Ley 1266 de 2008. *Diario Oficial No.48.587 del 18 de Octubre de 2012.* Bogotá: Juriscol.

Congreso de la República. (2011). *Ley No 29733.* Lima.

Congreso de la República. (18 de Octubre de 2012). Ley Estatutaria 1581 de 2012. *Diario Oficial No. 48.587 de 18 de octubre de 2012*. Bogotá: Juriscol.

Congreso de la República. (27 de junio de 2013). Decreto 1377. Bogotá: Presidencia de la República.

Constitución de la Nación Argentina (Asamblea constituyente Mayo de 1853).

Constitución de la República Bolivariana de Venezuela (Asamblea Constituyente Bolivariana 1999).

Constitución de la República Oriental del Uruguay (Parlamento Uruguayo 1967).

Constitución de la República portuguesa (Asamblea constituyente Abril de 1976).

Constitución Española (Congreso de los diputados Octubre de 1978).

Constitución Nacional del Perú (Congreso Constituyente Democrático 1993).

Constitución Política de los Estados Unidos Mexicanos (Congreso Constituyente 1917).

Corte Constitucional. (2011). C - 748 de 2011. *Control de Constitucionalidad de los Proyectos de Ley Estatutaria*. Bogotá: Corte Constitucional.

De la Calle Restrepo, J. (2008). *Autodeterminación informativa y habeas data en Colombia.* Bogotá: Temis.

Decreto 414 (Parlamento Uruguayo 2009).

Delgado Triana, Y. (2007). Protección en el ordenamiento jurídico cubano de los derechos inherentes a la personalidad en la esfera moral. Cuba.

Jefatura del Estado. (1999). *Ley Orgánica 15.* Caracas.

Ley 18.331 (Parlamento Uruguayo 2008).

Ley 1845 de Protección de Datos. (Legislatura de La ciudad Autonoma de Buenos Aires 2006).

Ley 25.326 (Congreso de la Nación 2 de Noviembre de 2000).

Ley del Censo. (1983). *Informática Jurídica.* Obtenido de Informática Jurídica: www.informatica-juridica.com/jurisprudencia/alemana.asp

Nieves Saldaña, M. (2011). El Derecho a la Privacidad en los Estados Unidos. *Teoria y Realidad Constitucional No 28*, 283.

Organizacion de Naciones Unidas. (10 de Diciembre de 1948). Declaración Universal de los Derechos Humanos. Paris: ONU.

Parlamento Europeo. (Octubre de 1995). Directiva 95/46/CE. *Protección de las Personas Físicas, en lo que respecta al tratamiento de datos personales y la libre circulación de los mismos*. Luxemburgo: Parlamento Europeo.

Parlamento Europeo. (2007). *Real Decreto 1720.* Madrid.

Piñar Mañas, J. (2006). *La Red Iberoamericana de Protección de Datos: Declaraciones y Documentos.* Valencia: Tirant to Blanch.

Prado, J. (2012). La Intimidad ¿Un derecho o un deber? de como el uso de las nuevas tecnologías Impacta la vida Personal. *Revista Javeriana*, 18 - 21.

Presidencia de la República. (2015). *Decreto 1074.* Bogotá.

Presidencia de la República. (2017). *Ley general de protección de datos personales en posesión de sujetos obligados.* Ciudad de México.

Presidencia de la República. (2018). *Decreto 090.* Bogotá.

Real Academia Española. (2014). *Diccionario de la Lengua Española.* Valencia: Real Academia Espanola, Edicion del tricentenario.

Remolina Angarita, N. (2013). *Tratamiento de Datos Personales, Aproximación Internacional y comentarios a la Ley 1581 de 2012.* Bogotá D.C.: Legis.

Resolución 509 (Consejo Europeo 1968).

Riccobono, F. (1991). il nouvo diritto del citadino. *nuovo diritti delléta tecnologica*, 6.

Rivera Llano, A. (2008). *Libertad Informática y Derecho a la autodeterminación informática.* México: Zlux.

Superintendencia de Industria y Comercio. (2015). Guía para la implementación del principio de la responsabilidad demostrada (Accountability). Bogotá.

Superintendencia de Industria y Comercio. (2017). *Cartilla Formatos Modelo Para el cumplimiento de la Ley 1581 de 2012 y sus decretos reglamentarios.* Bogotá D.C,: Industria y Comercio.

T - 022 (Corte Constitucional 1993).

T - 414 (Corte Constitucional 1992).

T - 440 (Corte Constitucional 2003).

T - 729 (Corte Constitucional 2002).

T - 729 (Corte Constitucional 2008).

Upegui Mejia, J. (2008). *Habeas Data, fundamentos, naturaleza, régimen.* Bogotá: Publicaciones Universidad Externado de Colombia.

Warren, S. y. (1980). Law rigtht to privacy. *Harvard Law Reviw*, 193 - 220.

Anexo 1: Encuesta

Según la normatividad vigente en lo referente a protección de datos personales, usted como usuario tiene derecho a rectificar, actualizar y conocer el propósito y destino de sus datos personales.

De acuerdo a lo anterior le pedimos conteste la siguiente encuesta con base en su experiencia:

¿Sabe usted que son datos personales?

SI NO

¿Conoce cuales se encuentran protegidos?

SI NO

¿Tiene usted conocimiento sobre la normativa y reglamentación para que sus datos personales se encuentren protegidos?

SI NO

¿Sabe cuál es la entidad autorizada para la inspección y vigilancia de protección en materia de datos personales?

SI NO

¿Cree usted que al momento de realizar una transacción y/o adquisición de algún servicio, sus datos personales se encuentran plenamente protegidos?

SI NO

¿ha sentido la vulneración en la protección de sus datos personales en ese sentido?

SI NO

¿Cree que su intimidad está siendo expuesta, cuando le piden sus datos personales en alguna entidad?

SI NO

¿Le ha ocurrido que una entidad diferente a la cual entregó sus datos personales inicialmente lo ha contactado con fines comerciales?

SI NO

¿ha sido usted víctima o conoce a alguien cercano, donde con ocasión a la mala administración de sus datos personales se haya cometido algún ilícito?

SI NO